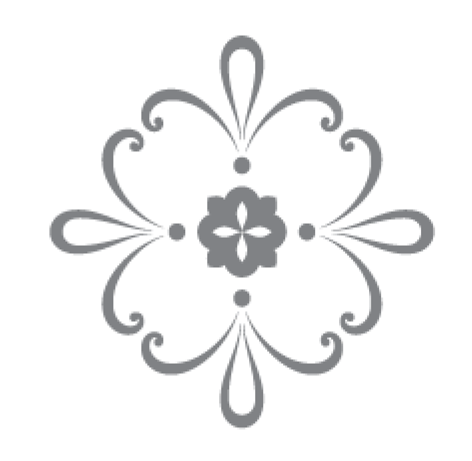
高等学校
科研保密管理体系建设

崔淑妮 主编



清华大学出版社

高等学校科研保密管理体系建设

崔淑妮　主编

清华大学出版社
北　京

图书在版编目(CIP)数据

高等学校科研保密管理体系建设/崔淑妮主编. —北京：清华大学出版社，2019
ISBN 978-7-302-52310-9

Ⅰ. ①高…　Ⅱ. ①崔…　Ⅲ. ①高等学校－科学研究工作－保密　Ⅳ. ①G644

中国版本图书馆 CIP 数据核字(2019)第 029194 号

责任编辑：朱玉霞
封面设计：常雪影
责任校对：王荣静
责任印制：丛怀宇

出版发行：清华大学出版社
网　　址：http://www.tup.com.cn，http://www.wqbook.com
地　　址：北京清华大学学研大厦 A 座　　**邮　　编**：100084
社 总 机：010-62770175　　**邮　　购**：010-62786544
投稿与读者服务：010-62776969，c-service@tup.tsinghua.edu.cn
质量反馈：010-62772015，zhiliang@tup.tsinghua.edu.cn
印 装 者：三河市金元印装有限公司
经　　销：全国新华书店
开　　本：160mm×230mm　　**印　　张**：19　　**字　　数**：260 千字
版　　次：2019 年 4 月第 1 版　　**印　　次**：2019 年 4 月第 1 次印刷
定　　价：69.00 元

产品编号：074525-01

前　　言

军民融合发展战略是习近平新时代中国特色社会主义思想的重要组成部分。深入贯彻军民融合发展战略是高校义不容辞的责任，是深化教育体制改革、推进高等学校“双一流”建设与发展的重要方略，也是实现“科技兴国”“科技兴军”目标的必由之路。伴随着军民融合科技创新步伐的不断推进，作为科技第一生产力、人才第一资源和创新第一动力的结合点，高校在服务经济社会、国防科技等方面发挥着重要的战略支撑作用，已成为科技创新、国防科研和军民融合工作的重要阵地和重要力量。

高校科研保密工作是高校国防科研发展的基石，是贯彻军民融合发展战略的重要保障，也是国家保密管理体系的重要组成部分。多年来，为了更有效地贯彻《武器装备保密资格审查认证（定）办法》，针对高校保密工作环境相对开放、场所较为分散、人员流动频繁、国际交往广泛等诸多特点，本书作者结合高校实际情况，对科研保密管理体系进行了系统研究，对所面临的诸多现实问题，做了大量有益的探索，形成了一定的研究成果，并将有关经验编撰成书。

本书依据国家保密法律法规及相关标准和规章制度的要求，结合高校科研工作的特点，提出高校保密工作责任体系、组织管理体系、工作制度体系与条件保障体系的建设标准，提供了高校科研保密体系建设可操作性范例，对推进高校科研保密管理工作规范化、流程化、精细化管理，特别是促进保密工作与科研业务工作深度融合，具有一定借鉴参考价值。

本书由清华大学崔淑妮等六位长期在科研保密管理岗位上工作的老师共同完成。全书共分十一章，其中，第一章由蒋东兴、徐娟编写，第二章由崔淑妮、徐娟编写，第三、五、七、九、十、十一章由崔淑妮编写，第四章由杨芳、崔淑妮编写，第六章由龙平编写，第八章由苗春雨编写，由崔淑妮负

责统稿、审定。希望借此与广大保密干部和涉密人员，特别是从事科研涉密与管理工作的人员分享经验与成果，促进高校科研保密工作整体水平的提高，切实为新时代军民融合深度发展工作提供坚实保障，为我国高等教育事业的发展和强国强军目标的实现做出新的更大贡献。

限于作者水平，书中难免存在疏漏和不当之处，恳请同行和读者不吝指正。

编　者

2018 年 12 月

目　　录

第一章　绪　　论

人才培养、科学研究、社会服务、文化传承创新是新时期我国高等教育的四大功能。组织高校师生及科技人员开展科学研究、技术开发和社会服务工作，是高校的一项重要工作。特别地，随着军民融合科技创新步伐的不断推进，高校承担了越来越多的武器装备科研生产任务。因此，做好军工科研项目的保密管理工作，对高校的保密工作提出了新的更高的要求。

一、高校科研保密的相关概念

（一）高校科研工作

科研是科学研究的简称，一般是指利用科研手段和装备，为了认识客观事物的内在本质和运动规律而进行的调查研究、实验、试制等一系列的活动，为创造发明新产品和新技术提供理论依据。根据研究工作的目的、任务和方法的不同，科学研究通常划分为以下几种类型。

（1）基础研究：是对新理论、新原理的探讨，目的在于发现新的科学领域，为新的技术发明和创造提供理论前提。

（2）应用研究：是把基础研究发现的新的理论应用于特定的目标的研究，它是基础研究的继续，目的在于为基础研究的成果开辟具体的应用途径，使之转化为实用技术。

（3）开发研究：又称发展研究，是把基础研究、应用研究成果应用于生产实践的研究，是科学转化为生产力的中心环节。

基础研究、应用研究、开发研究是整个科学研究系统三个互相联系的环节，它们在一个国家、一个专业领域的科学研究体系中协调一致地发展。科学研究应具备一定的条件，如需有一支合理的科技队伍、必要的科研经费、完善的科研技术装备以及科技试验场所等。

高校作为国家科研系统的重要组成部门，具有学科和人才方面的优势，承担了大量的科研项目，完成了大量的科研成果，积聚了科学技术的巨大潜力，是发展科学技术的重要基地。

（二）高校科研管理

高校科研管理按照科学技术和高等教育发展规律以及管理学原理，在科研过程的各个环节对学校科研活动中的人、财、物、时间、信息和效果等进行计划、组织、控制和总结，包括学校科研发展规划和管理制度的制定、实施以及科研项目管理、科研组织、科研效应评价等诸多方面。高校科研管理是对科研活动的全过程管理，具体管理要素包括科研机构、科研人员、科研项目、科研经费、科研成果、科研评价和科研档案等。

高校科研既有科学研究的共性特点，又具有高校自身的特色，因此高校科研管理必须考虑如下特点。

（1）高校科研具有多学科、多专业的特点。

（2）高校科研以理论研究和实验室研究为主。

（3）高校的科研团队担负着科研和教学（培养人才）双重任务。

（4）高校的科研方向围绕重点学科和学科带头人的专业研究方向展开。

（5）受人才结构、专业特点和研究积累等影响，高校科研各学科发展不均衡。

（6）高校科研中人文社科和理工科有较大差别。

（7）高校科研的社会触角较为广泛，国内国际交流非常活跃。

（三）科研保密管理

武器装备的科学研究关系国防安全和国家安全。随着国家军民融合

发展战略的大力实施，很多高校积极参与国防科技研究，承担了越来越多的国防科研任务，已成为国家国防科研的重要力量。特别是近年来，高校承担了许多国家重大国防科研专项任务，一旦发生失密、泄密事件，会给国家造成巨大的损失，直接关系学校的发展、社会的稳定和国家的安全。随着高校在承担国防科研任务的过程中担负的保密责任越来越重，做好科研保密管理，已成为高校的重要工作之一。

高校承担国防科研任务，一般以项目（课题）的形式委托给相关的国防科研项目组（课题组），项目组是高校国防科技创新的基本单元。从过程管理的角度来看，国防科研项目大致可以分为三个阶段：项目的前期阶段（规划建议与论证申报）、中期阶段（立项与实施）、后期阶段（结题验收与成果管理）。

保密工作与国防科研项目实施的全过程密切相关，保密管理贯穿于项目前期研究、规划建议、申报、立项、实施、结题、验收等全过程，科研过程的各个环节要与保密措施的实施同步进行，每一个环节都应当处在规范的保密监督管理中。

为了切实做好高校科研保密管理，必须建立高校涉密科研项目保密工作体系，包括组织体系与制度体系。高校科研保密工作体系的建立，必须遵循《中华人民共和国保守国家秘密法》及其实施条例、《国家秘密定密管理暂行规定》《武器装备科研生产单位保密资格审查认定办法》等法律法规和规章制度。

二、高校科研保密管理要素

科研工作可以抽象为：科研人员在科研场所、利用科研设备和载体开展一系列科研活动，从而取得科研成果。科研保密管理要实现涉密科研工作全过程的国家秘密管理，必须围绕科研工作的以下要素展开。

（一）科研人员

科研人员是科研工作中最为重要的要素，是国家科技秘密的直接生产

者，因而也是科研保密管理的第一要素。因此，涉密人员管理一直是保密监督管理的核心内容。

涉密科研人员既是直接参与国家技术秘密的第一知情者、保护者，也可能是国家秘密知悉范围的擅自扩大者、泄密的直接责任人。从发生过的科研泄密案件来看，大多都是由科研人员造成的，除极个别是当事人利欲熏心外，绝大多数都是由于科研人员不重视保密工作，保密意识和保密能力不足造成的。对于高校来说，科研人员除了高校教师外，还有博士生、硕士生甚至本科生，近年来合同制科研人员参与涉密科研项目也越来越多，高校涉密科研人员组成越来越复杂。同时，由于高校开放办学的思想影响根深蒂固，高校师生总体来说保密意识不强、保密能力不足。

因此，科研人员保密管理首先就是要加强保密宣传教育，增强科研人员的保密意识和保密技能，使科研人员了解科研保密的重要性，主动做好保密工作，成为国家科技秘密的自觉保护者。由于高校人员类型较多，还需要对人员按照涉密程度进行分类，如分为普通教师、普通学生、涉密科研人员、涉密管理人员、党政干部等，对于不同类型的人员需要采取不同的保密宣传教育方式和内容。

针对涉密科研人员，还必须建立一整套涉密人员保密管理制度，包括涉密岗位和涉密等级的确定、涉密人员资格审查与密级界定、岗前培训与在岗保密教育培训、保密自查、出国(境)与涉外活动管理、离岗与脱密期管理以及保密补贴与考核奖惩等。

（二）科研场所

科研场所是科研活动发生的主要场所，也是科研成果产生和保存的主要场所，更是科研设备和载体存放的集中场所。因此，对于涉密科研项目来说，科研场所也是非常重要的保密管理要素。

在高校中，科研场所的范畴非常广泛，既包括仪器设备集中存放的实验室，也包括研究人员日常工作的办公室，还包括试验车间、会议室、资料室等。由于高校承担国防科研任务的项目组往往同时承担着不涉密的其

他科研项目，因此涉密科研任务和非涉密科研任务常常在同一个科研场所进行，这给科研场所的保密管理带来了更大的挑战。

为了做好科研场所的保密工作，首先，要根据国防科研项目的具体研究情况，清晰界定哪些科研场所将会产生、存储、保管国家秘密，进而将这些场所明确定义为涉密科研场所，实施严格的保密管理。

其次，对涉密场所进行分类管理，根据涉密程度及用途的不同，采取不同的保密管理措施。其中，保密要害部门、部位的管理是重中之重：要将学校科研、生产、管理等工作中产生、传递、使用和管理绝密级或较多机密级、秘密级国家秘密的内设机构确定为保密要害部门；将学校各单位内部集中制作、存储、保管绝密级国家秘密载体或较多机密级、秘密级科研项目文件、资料、成果等国家秘密载体的最小的专用、独立、固定场所，以及承担较多机密级以上或大量秘密级武器装备相关项目的研制、生产、试验场所，确定为保密要害部位。对保密要害部门、部位需要制定明确的规章制度和标准要求来实施管理，包括确定、变更和撤销的程序，人防、技防和物防保障标准以及日常保密保卫管理制度等。此外，对于其他涉密场所，如涉密实验室、涉密会议室、涉密档案室、涉密外场试验场地等，也必须分别提出相应的保密管理要求。

（三）科研设备与载体

科学研究离不开科研设备和载体。科研设备是指科学研究过程中所使用的各种设备和仪器等，是科研工作中知识和技术创新的重要工具，也是科研单位实力的重要标志。载体是信息传播中携带信息的媒介，是信息赖以附载的物质基础，即用于记录、传输、积累和保存信息的实体，包括以能源和介质为特征，运用声波、光波、电波传递信息的无形载体和以实物形态记录为特征，运用纸张、胶卷、胶片、磁带、磁盘传递和储存信息的有形载体。可以说，涉密科研项目中的国家秘密，都离不开科研设备和载体，因此，涉密设备和涉密载体的管理同样是保密监督管理的重点之一。

高校承担的国防科研任务，以基础研究类、技术研究与开发类项目为

主,较少承担工程研制类项目。因此,除了少量专用涉密科研设备需要特殊保密管理外,重点要考虑的是通用涉密科研设备的管理,特别是广泛使用的涉密信息设备的管理,如计算机、通信设备、办公自动化设备等。由于计算机、通信和办公自动化设备在高校的广泛联网使用,因此,高校的科研设备保密管理不能只关注涉密设备,对非涉密的联网设备也要重点给予监管,要制定严格的措施确保国家秘密不会流入联网设备。

在科研载体方面,由于高校广泛使用移动存储介质,如移动硬盘、U 盘、光盘和存储卡,使得国家秘密载体的保密管理难度很大,是保密监督管理的重点之一和长期难点所在。因此,为加强管理控制,确保涉密载体安全,需要在以下方面开展工作。

(1) 加强对涉密文件资料等纸质涉密载体的管理,在做好台账管理的基础上,严格按照有关规定做好制作与复印、收发与传递、保管与维修、使用与归档等工作。

(2) 严格管理磁介质、光介质和半导体介质的各类涉密移动存储介质,尽量采用统一采购的涉密 U 盘和光盘,定期清查核对各单位的涉密移动存储介质台账,严禁涉密移动存储介质接入非涉密计算机。

(3) 规范涉密载体的报废处理,对批准销毁的国家秘密载体实施统一管理并集中销毁,严防使用者私自降密处理。

(四) 科研活动

科研活动是科研过程中科研人员发生的各类研究活动,包括查阅资料、科学试验、科学计算、数据处理、会议讨论、撰写论文等。在国防科研中,国家秘密将贯穿于各种科研活动,是科研活动的重要信息来源,同时科研活动也会产生新的国家秘密。因此,做好科研活动的保密管理,对科研保密管理至关重要。

但困难的是,活动是一个动态的系统,特别是对于高校的科研人员来说,同一个时期会开展各种不同的科研活动,这些科研活动可能属于不同的科研项目,有些涉密而有些不涉密,这给科研人员做好保密工作带来了

很大的困扰。

要做好科研活动的保密管理，首先，科学规范定密是基础。只有准确确定国防科研项目中的保密要点，明确需要保密的项目内容，才能有针对性地做好相关科研活动中的国家秘密的保密管理。

其次，要根据不同的科研活动性质，制定不同的保密管理细则，如涉密项目学术交流保密管理细则、数据处理保密管理细则等。对于一些有较多共性的科研活动，可以制定校级层面的保密管理办法，如涉密会议保密管理办法、涉外活动保密管理办法、外场试验保密管理办法和协作配套保密管理办法等。

此外，高校的涉密科研活动还有两条明确的线索，一条是涉密科研项目，另一条是涉密研究生学位论文，这两条线索把高校两类主体涉密科研人员所开展的科研活动有机地串联起来。因此，对于高校来说，建立涉密科研项目保密管理办法和涉密研究生论文保密管理办法等专项保密管理制度，对两大类科研活动实施全过程的保密管理，是一种值得借鉴的保密管理思路与措施。

（五）科研成果

科研成果是科研人员在其所从事的某一科研项目或课题研究范围内，通过实验观察、调查研究、综合分析等一系列脑力、体力劳动所取得的、并经过评审或鉴定，确认具有学术意义和实用价值的创造性结果。科研成果的形式多种多样，既可以是应用模型、学术论文、咨询报告、建议、方案、规划，也可以是技术专利、计算机软件、程序，还可以是科研新理论、新方法及其科研设计、新产品的工艺流程、图表、数据等。对于国防科研来说，国家秘密主要就包含在科研成果中，因此做好科研成果的保密工作对国防科研保密管理具有重要意义。

在高校中，科研成果保密最大的难点在于定密，因为高校科研工作大多具有军民两用的特点，要想准确判断科研成果中的科技信息是否涉密存在一定的困难。特别是由于高校开放的科研氛围浓郁，“科学没有国界，科

研成果应该完全公开和共享”的思想被很多科研人员奉为圭臬，一般科研人员很少会考虑科研成果的保密问题，这对国防科研成果的保密管理提出了很大的挑战。

因此，要做好高校科研成果的保密管理，科学规范的定密工作仍然是重要基础。在此基础上，严格执行涉密载体管理办法，确保承载了涉密科研成果的载体准确标密、规范管理、合法利用。此外，还要把握好科研成果的对外发布与宣传关口，制定严格的宣传报道保密管理办法，做好发表论文、申请专利和出版学术专著等的保密审查，确保国家秘密不从科研成果的发布途径中泄露。

三、高校科研保密体系

高校的科研保密工作，就是要围绕前述的五类保密管理要素展开：建立针对各类要素的保密管理制度和保密监督检查与奖惩制度，形成完善的覆盖涉密科研任务研究过程各个环节的保密管理制度体系；建立保密组织体系和保密工作责任制，落实机构和人员，明确职责权利，确保保密管理制度体系的规范实施。通过保密管理制度体系和组织体系的建立，形成能够保障国家秘密安全的高校科研保密体系，其构成要素如图 1-1 所示。

（一）保密制度

保密制度是指一个国家、单位或团队在从事保密管理活动中，根据活动内容的不同，将不对外公开的信息资料及内容进行保密而制定的法律、法规，构成制约相关人员共同遵守的保密规则或行为规范。对高校科研保密工作来说，保密制度是为了在完成所承担的国防科研任务的同时也保守好国家秘密而制定的具体办法与措施，是保密法律法规和规章制度在学校的具体化，是学校师生从事保守国家秘密活动最直接的规范和依据。

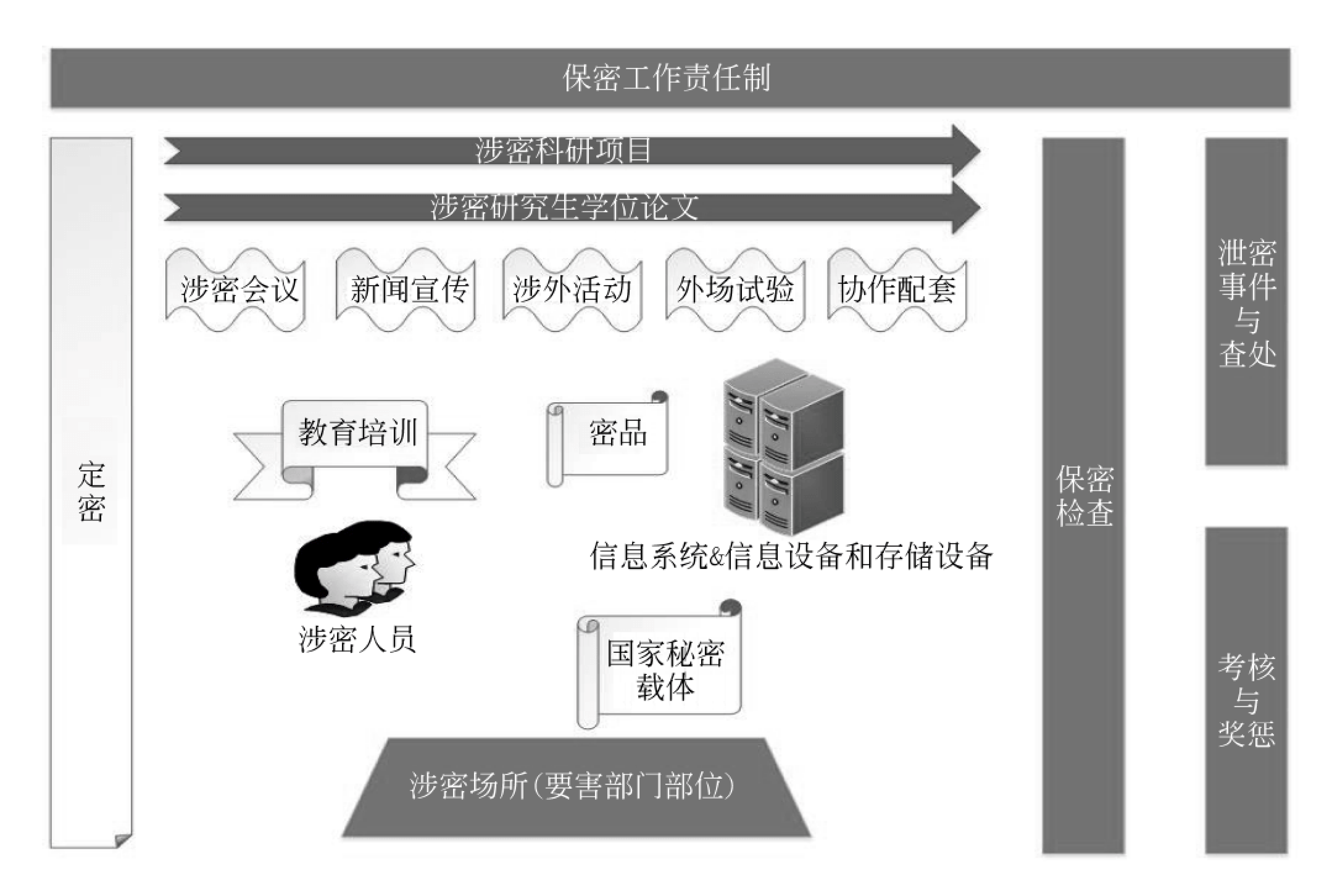


图 1-1 高校科研保密体系示意图

一般来说，高校为了保守国防科研中的国家秘密，需要制定并执行如下保密制度。

1.《保密工作管理规定》

《保密工作管理规定》作为学校保密工作的基本依据，一般由学校保密委员会组织制定，经学校党委常委会或校务会议审核后发布。主要用于明确学校保密工作的方针，确定学校保密管理组织体系与保密工作责任，规定学校保密工作的范围、内容和要求以及保密工作中的责任追究与奖惩等。

2. 保密基本制度

根据《武器装备科研生产单位保密资格标准》要求，承担国防科研任务的高校必须建立的基本制度包括：明确学校各级领导干部、涉密人员和有关部门保密管理职责的保密责任制；为各项保密监督管理提供基础依据的定密工作管理办法；针对从事涉密科研、管理工作人员的涉密人员管理办法和保密教育培训管理办法；针对科研场所的保密要害部门、部位管理办

法;针对科研设备与密品密件的信息系统、信息设备和存储设备保密管理办法;国家秘密载体与密品保密管理办法;针对科研活动的涉密会议管理办法、协作配套保密管理办法、涉外活动保密管理办法、外场试验保密管理办法;针对科研成果的新闻宣传保密管理办法,以及保密检查工作实施办法、泄露国家秘密事件报告和查处管理办法、保密工作考核与奖惩管理办法等保密监督检查与奖惩制度。

基本制度由学校保密工作机构组织制定,经学校保密委员会审核后,由学校法定代表人或主要负责人签发。

3.《涉密科研项目保密管理办法》

对承担国防科研任务的高校来说,涉密科研项目的保密管理就成为学校保密监督管理中分量最重的工作。与项目管理紧密结合,将保密管理贯穿于项目规划建议、申报论证、立项、实施、验收、资料归档、成果鉴定、经费管理等全过程,是高校抓好科研保密管理的重要经验。因此,制定《涉密科研项目保密管理办法》业务制度,明确学校涉密科研项目保密管理的原则,确定科研机构、科研人员和有关部门的工作职责,规定科研项目全生命周期各个环节的保密要求,能够起到纲举目张的作用。

4.《研究生学位论文保密管理办法》

研究生是高校科研工作的重要力量,也是高校科研工作中最活跃且流动性最大的人群。研究生参与涉密科研项目也给高校科研保密管理带来了很大的挑战。一般来说,研究生参与涉密科研工作大多是因为学位论文研究的需要,因此,以研究生学位论文为抓手来推动涉密研究生的保密管理,制定《研究生学位论文保密管理办法》业务制度,从学位论文研究的全过程进行管理,规定学位论文研究各个环节的保密要求,明确有关管理部门的工作职责,具有提纲挈领的作用。

此外,还可以根据学校科研工作实际情况需要,制定《涉密地质资料使用保密管理办法》《涉密设备采购与管理保密实施办法》等其他专项保密制度。对于承担涉密科研任务的具体院系或课题组,则可以根据保密工作实际情况,制定更有针对性的保密管理二级制度。

（二）保密组织

保密组织是行政组织的重要组成部分，是指依照国家法律、法规的规定，在贯彻保密管理方针、实施保密管理目标的行政管理过程中，为确保国家秘密安全、科学管理国家秘密，通过分配任务、建立责权体系，对保密机构行政人员所做的安排，是具有明显层级特征和结构形式的相对稳定的系统管理集体。保密工作组织机构一般分为领导机构和管理机构，对于高校来说，就是保密委员会和保密管理办公室。

保密委员会作为学校保密工作的领导机构，主管学校保密工作，其主任应由学校负责人担任，成员包括有关部门（如党政、教学、科研、组织人事、宣传、外事、财务、信息、保密、保卫等）的主要负责人，同时成员应有明确的职责分工。按照《武器装备科研生产单位保密资格标准》要求，保密委员会应当实行例会制度，对学校保密工作进行研究、部署和总结，及时解决保密工作中的重要问题。

保密管理办公室作为保密委员会的日常办事机构，负责组织协调、指导、监督、检查学校保密工作。按照《武器装备科研生产单位保密资格标准》要求，一级资格单位涉密人员 100 人（含）以上或二级资格单位涉密人员 200 人（含）以上的，学校必须设置负责保密管理工作的专门处室，在保密委员会领导下独立行使保密管理职能，专门从事保密管理工作。

实际上，对于承担了国防科研任务的高校来说，为了进一步把保密管理落到实处，除了校级的领导机构和管理机构外，还会在二级机构（院系部处）和具体承担国防科研项目的基层单位（如研究所、实验室、课题组、项目组等）设置保密工作管理机构或岗位，协同配合、共同承担保密管理工作。

四、高校科研保密工作难点

高校的科研保密工作不同于其他科研生产单位，面临着许多复杂的情况，有许多特殊性，如高校与校外和境外联系紧密，学术交流频繁；有大量

的学生参加科研工作，教师和学生流动性都很大，并且科研人员撰写的论文数量较多；科研工作分散于各个院系，参与国防科研的人员、场所和设备也很难与普通的教学科研分开。这些特殊性使高校保密工作面临的环境更加复杂，也是高校科研保密管理的工作难点。

（一）环境开放、场所分散

开放性和国际化办学是高校为了适应世界形势和自身发展需要的重要举措，开展国际科技交流与合作是科学技术不断发展的客观要求和必要条件。因此，高校的国防科研保密也将毫不例外地与科技开放并存，这构成了高校科技保密环境的开放性。

此外，大部分高校没有统一的涉密科研场所，涉密项目的研究场所往往分散在学校的不同位置，并且多数项目组由于受物理空间限制，涉密项目往往与非密项目共用研究场所，涉密场所和非涉密场所交叉、涉密计算机和非涉密计算机同置一室的情况非常普遍，这给保密管理和防护增加了不小的难度。

（二）科研人员项目交叉、流动大

高校科研任务重，承担涉密科研项目的科研人员和研究生往往同时承担非涉密项目，并且参与涉密科研项目的博士、硕士和本科生数量较大，毕业后流动性强。同时，高校涉密科研项目资料和涉密学位论文的管理和归档问题较为复杂，这形成了高校涉密科研项目人员、资料管理难度大的局面。

此外，高校对外交流广泛，科研人员出国留学、访问及参加学术会议较多，同时高校与国外的大学互访频繁，还招收大量的外国留学生，形成了动态的人员国际交流和流动的局面，这种开放活跃的学术氛围对高校科研保密工作提出了更高的管理要求。

（三）学校文化崇尚自由与创新

高校科研人员思维发散，创新性强，崇尚自由，主要通过参加学术研讨会、发表学术论文等学术交流活动向同行展示学术成果以获得学术声誉，

因而频繁参加国内外学术交流,发表大量论文、著作。高校师生长期生活工作在和平环境,对保密工作的残酷性缺乏体验,敌情意识较淡漠,容易滋生麻痹思想,稍有不慎就会发生泄密事件。

此外,高校属知识密集型单位,新技术、新设备应用超前,信息化程度高。师生大量使用笔记本电脑、U 盘、移动硬盘、手机存储卡等新型设备载体,网络四通八达,计算机数量大,并且大量自建的局域网与国际互联网相连,使得泄密渠道增多。

五、高校科研保密管理思路

根据高校国防科研工作特点和保密管理难点,需要有创新性的保密管理思路,有针对性地解决高校科研保密问题,构建高校国防科研保密管理的长效机制。

(一) 建立总体开放、国防科研局部封闭格局

高校的特点和国防科研的要求具有强烈的不兼容性(见表 1-1),要做好高校的国防科研保密工作,必须按照国防科研的要求对高校进行适当改造。权衡高校的长远发展与国防科研的长治久安,建立总体开放、国防科研局部封闭的高校国防科研格局,是一个可以兼顾两方面的解决方案:总体开放能够保护高校科研的活力,局部封闭可以保障国家秘密的安全。

表 1-1　高校特点与国防科研要求

要素	高校特点	国防科研要求
环境	开放	封闭
场所	分散	集中
人员	交叉、流动	稳定
管理	粗放型	精细化
文化	自由、创新	服从、规范

局部封闭可以有两种模式，一种是以学校为主体的局部封闭模式，另一种是按院系局部封闭的模式。

学校为主体的局部封闭模式是指学校建立实体的国防科技研究机构，如北京大学和浙江大学建立的先进技术研究院，作为从事国防科技研究与管理的实体机构。实体国防科技研究机构可以采用较为灵活的运行机制和特殊的管理政策，包括与国防科研相适应的经费管理和人员评估政策，整合学校在国防科技方面的科研队伍，加强项目的组织和管理，提升学校承担国防科研项目和保密管理的能力。

按院系局部封闭的模式是指以院系作为学校承担国防科研和保密管理的主要机构，在从事国防科研的院系建立相对集中、封闭的国防科研场所和二级机构保密体系，院系是其所承担国防科研项目的保密管理责任主体。清华大学等多数承担国防科研任务的高校采用了按院系局部封闭的模式。这种模式的优点是比较灵活，可以根据院系承担国防科研项目的情况逐步扩展国防科研体系与保密体系建设；缺点是对于国防科研项目较少的院系来说，建立本院系的国防科研场所和二级机构保密体系代价较大、难度较高。

两种模式也可以综合采用，即在学校为主体的局部封闭模式基础上，对于特殊的或新增的国防科研项目采用按院系局部封闭的模式。无论采用何种模式，关键是要使得从事国防科研项目的人员、设备、载体、场地相对集中，落实国防科研保密工作的责任制和全过程的管理，确保国家秘密的安全。

（二）建立校、院系、项目组三级保密管理体系

在高校中，院系是相对独立的教学、科研实体机构，负责本院系的教学、科研、人事、财务、设备资产等的统一管理；而项目组（课题组）是高校科技创新的基本单元，一个科研任务的完成，其主要科研活动都在项目组（课题组）范围内开展，国防科研涉及的国家秘密也主要在项目组（课题组）内流转。因此，要做好国防科研的保密管理工作，可建立校、院系、项目组三

级保密管理体系，三个层面分工负责、协同配合，共同完成保密工作。

学校层面的机构一般包括保密领导机构（保密委员会），主管全校保密工作，组织制定学校的保密规章制度、审批决策学校保密工作重要事项；保密管理机构（保密管理办公室），作为保密委员会的日常办事机构，负责组织协调、指导、监督、检查学校的保密工作。

院系层面要设立保密工作领导小组，作为院系保密管理责任主体，负责组织、协调、监督、检查本单位涉密项目的保密工作，并为本单位开展涉密项目保密工作提供必要的组织保障和条件保障。院系保密工作领导小组由各院系负责人担任组长，成员应包括本单位负责科研、党务、机要文件、研究生、外事、档案、信息化等工作的管理人员。院系还需要设置专/兼职保密员负责本单位的日常保密管理工作，设置专/兼职计算机安全保密管理员负责本单位涉密人员使用信息设备的日常保密管理工作。

项目组（课题组）层面主要是要明确并落实项目（课题）负责人的保密责任，规定涉密科研项目负责人为保密工作负责人，对本项目组的保密工作承担直接领导责任。对于大型项目组，可以设置专/兼职保密员和计算机安全保密管理员协助项目负责人开展日常保密管理工作。此外，对于项目组来说，明确规定并落实涉密人员在科研活动中的保密责任也是抓好保密管理的重要工作。

（三）“抓源头、抓核心、抓重点、抓关键”

高校科研保密工作任务繁重、形势复杂、千头万绪，抓住国防科研保密的主要矛盾和矛盾的主要方面对于保密工作非常重要。因此，以项目负责人为源头，以定密为核心，以涉密区环境建设、涉密信息系统、信息设备和存储设备管理、涉密载体管理为重点，以领导为关键，建立保密管理长效工作机制，是做好高校科研保密工作的重要方法。

由于高校承担国防科研任务一般是以项目（课题）的形式委托给相关的国防科研项目组（课题组），因此科研保密工作的源头就是涉密项目及其负责人。项目负责人全面掌握着项目的涉密事项情况，总览项目研究全

局，因此，加强项目负责人的保密教育，明确项目负责人的保密责任，提高项目负责人的保密意识和保密能力，并督促项目负责人在项目研究过程中实施全程同步的保密管理，是做好国防科研保密工作的重中之重。

保密工作保的是国家秘密，只有把国家秘密定准了，保密工作才有明确目标，保密措施才能有针对性地落实。在科研保密管理工作中，定密是涉密人员管理、国家秘密载体管理、涉密计算机与信息设备管理的基础。因此，落实定密责任人制度，规范定密依据和国家秘密确定过程，做好国家秘密标志，完善国家秘密变更与解除机制，是做好国防科研保密管理的基础性工作。

高校在从事国防科研工作时，涉密信息集中在涉密科研人员、涉密科研场所与档案室、涉密信息设备和存储介质中，因此，除了涉密人员特别是项目负责人的管理是重中之重外，涉密区特别是保密要害部门部位的环境建设与防范、涉密信息设备和存储设备的管理，以及涉密载体包括各类存储介质的管理，是高校科研保密工作中需要常抓不懈的重点工作。

保密工作从根本上来说还是人的工作，因此，各类人员特别是领导干部对于保密工作的重视，是做好保密工作的关键。要严格落实各级党政领导干部保密工作责任制，领导干部要自觉学习、及时传达上级的保密工作文件和指示，不断提高思想认识；要自觉接受保密监督，模范遵守保密法律法规和各项保密制度，带头贯彻执行上级关于保密工作的方针、政策、指示、决定，及时了解保密工作情况，进行督促检查，及时发现和解决存在的问题；此外，还要积极为保密部门和保密干部做好工作创造必要条件，支持保密管理队伍依法依规开展工作。

第二章　保密工作组织机构

保密工作组织机构是高校开展科研保密工作、落实保密管理要求的基本保障。保密组织机构建设关键是组织健全、人员到位、责任落实。

一、高校保密工作组织机构

承担武器装备科研生产任务的高校通常建立党委领导下的校、院系部处、基层单位（主要指研究所、实验室、课题组、项目组等）完整的三级保密工作管理体系。组织机构图参见图 2-1。

（一）校级保密组织机构

校级保密组织机构包括保密委员会与保密工作机构。高校保密工作机构一般以保密管理办公室、保密委员会办公室、保密处等形式设置。

1．保密委员会职责、分工与工作规则

保密委员会作为高校保密工作的领导机构，其职责主要包括以下内容：

（1）贯彻落实中央关于保密工作的方针政策、党的保密纪律和保密法律法规。

（2）组织落实学校党委关于保密工作的决定，为学校决策解决保密工作重大事项提出建议。

（3）组织审定学校保密规章制度。

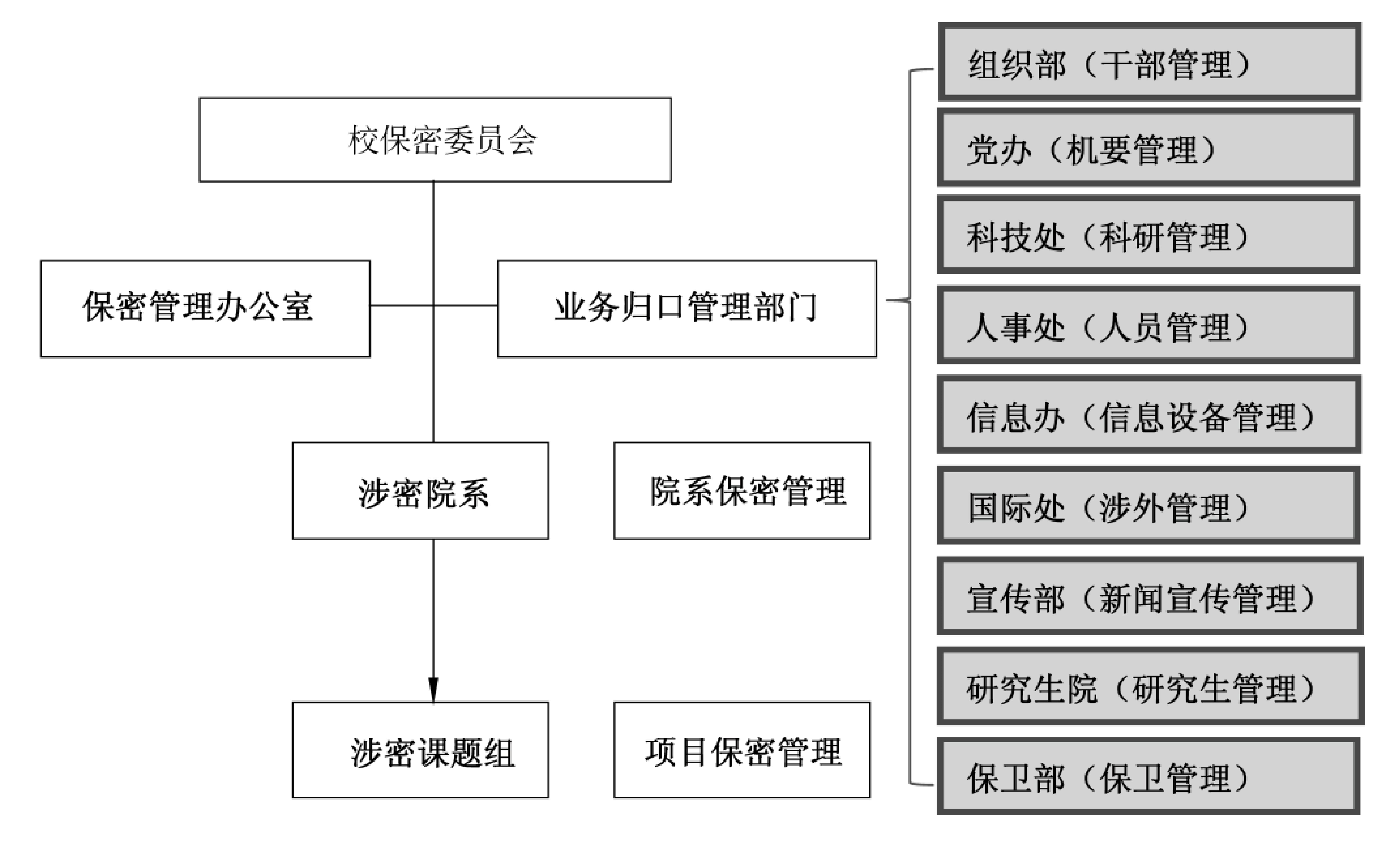


图 2-1　高校保密组织机构图

（4）研究部署学校保密工作。

（5）审查审批学校保密工作重要事项。

（6）组织检查学校保密工作开展情况。

（7）组织查处失泄密事件。

（8）表彰奖励保密工作先进单位和个人，组织调查相关违规违纪行为并提出责任追究和处理意见。

（9）落实上级机关和学校领导交办的其他工作。

高校保密委员会领导（含主任、副主任）一般由校领导兼任，成员包括有关部门（如党政、教学、科研、组织、人事、宣传、外事、财务、信息、保密、保卫等）的负责人（含正职或副职）。随着高校承担涉密科研任务的增多，为落实保密工作责任，特别是《武器装备科研生产单位保密资格标准》进一步强调法定代表人或主要负责人的责任，很多高校由党委书记或校长担任保密委员会主任，主管科研、人事、信息化的校领导任副主任，与科研保密密切相关的重点部处与院系正职领导担任保密委员会委员。保密委员会领

导与主要成员分工参见表 2-1。

一级保密资格单位依照有关规定还应当设立保密总监，一般由常务副主任兼任，其主要职责是协助保密委员会主任组织开展学校保密工作。

表 2-1　保密委员会领导与主要成员职责分工

保密委员会组成	职　务	职 责 分 工
主任	校党委书记/校长	全面领导学校保密工作
常务副主任	校党委副书记/副校长	分管全校保密工作
副主任	主管科研/人事/信息副校长	主管领域全校保密工作
主要成员	党办主任	机要保密工作
	保密办主任	保密管理办公室全面工作
	科技处处长/国防院院长	科研/国防项目的保密工作
	人事处处长	涉密人员保密管理
	信息办主任	信息系统、信息设备与存储设备保密工作
	保卫部部长	保卫保密工作
	重点涉密院系正职领导	所在院系保密工作

为了保证保密委员会切实履行职责，按照《武器装备科研生产单位保密资格标准》，保密委员会应当实行例会制度，通常每学期召开一次保密委员会工作例会，及时研究、部署和解决学校保密工作重大事项。根据实际需要，保密委员会可以组织召开主任会或专题会议，及时研究学校保密工作中的重要问题，提出加强和改进保密工作的措施与意见。

为了规范保密委员会的工作，确保保密委员会的例会效果，应当制定明确的工作规则(参见附件 2-1)。明确会前准备事项、参会人员范围、会议主要议题以及会议记录要求等。保密委员会成员应当及时传达保密委员会的会议精神并按职责分工组织贯彻执行。

保密委员会成员应当根据职责分工组织开展调查研究，对保密工作存在的实际问题和困难，提出加强和改进学校保密工作的措施和方法，联系督导

所在单位及相关主管业务保密管理工作，督办保密委员会决定的事项。

为了保证保密委员会成员能够切实履行职责，每年年底，保密委员会成员应当通过述职、述密等方式向保密委员会书面报告履职情况。述职方式可与年度干部述职结合进行，在述职报告中包含保密工作履职情况，述密方式是结合分管业务工作，向保密委员会专门报告保密工作开展情况。

2. 保密工作机构职责、人员要求与工作要求

作为保密委员会下设的日常工作机构，高校保密工作机构负责组织协调、指导、监督、检查学校保密工作。它的职责主要包括以下内容：

(1) 落实学校有关保密工作的要求，组织落实保密委员会的工作部署。

(2) 起草学校年度保密工作计划，对保密工作的具体落实提出意见建议。

(3) 组织起草学校保密规章制度。

(4) 监督指导各单位保密管理工作。

(5) 组织确定和调整保密要害部门部位。

(6) 组织开展保密检查。

(7) 具体组织调查失泄密事件及相关违规违纪行为。

(8) 提出保密责任追究和奖惩建议。

(9) 落实上级机关以及学校交办的其他工作。

为了确保保密工作机构独立行使保密管理职能，《武器装备科研生产单位保密资格标准》对保密工作机构与人员的配备提出了明确的要求：涉密人员100人(含)以上的一级保密资格单位或涉密人员200(含)人以上的二级保密资格单位，学校应当设置负责保密管理工作的专门处室，配备专职领导，级别为正处级。对不足100人的一级保密资格单位或不足200人的二级保密资格单位以及三级保密资格单位，可不设独立处室，但必须确定一个部门负责保密管理工作，在保密委员会领导下独立行使保密管理职能。对一级保密资格单位，涉密人员数量1000人(含)以上的，专职保密工作人员不得少于4人(含专职领导)；500人(含)以上至1000人以下的，专职保密工作人员不得少于3人；100人(含)以上至500人以下的，专职保密工作人员不得少于2人；100人以下的，专职保密工作人员不得少于1人。

对二级保密资格单位，涉密人员数量 1000 人(含)以上的，专职保密工作人员不得少于 3 人；200 人(含)以上至 1000 人以下的，专职保密工作人员不得少于 2 人；200 人以下的，专职保密工作人员不得少于 1 人。对三级保密资格单位，涉密人员数量 100 人(含)以上的，专职保密工作人员不得少于 1 人；100 人以下的，应配备兼职保密工作人员。以上人数要求是专门针对学校保密工作机构提出的，不包含学校所属各单位配备的专职保密工作人员。

保密工作机构(以下以保密管理办公室为代表加以说明)专兼职保密工作人员除了要求具备良好的政治素质，具有一定的管理能力，还应当熟悉学校和保密工作情况，熟悉保密法律法规，掌握保密知识技能，通过上级主管部门或专业机构组织的保密知识技能培训。

为了适应信息化条件下保密管理工作的要求，专职保密工作人员 2 人以上的高校，应当配备 1 名保密技术管理人员，负责指导、监督和检查学校保密技术防范措施建设和管理。保密技术管理人员应当接受相关计算机网络或信息技术专业学习或培训，熟悉国家有关保密法规与保密工作相关的各类信息安全技术防范知识。

为了确保高校保密工作有序开展，每年年初保密管理办公室应当依据本地区、本行业年度保密工作要点以及学校具体情况制订年度保密工作计划，一般包含拟开展主要工作、计划完成时间等信息(参见附件 2-2)，提交保密委员会审议。通过后，下发学校所属各单位，并组织各单位制订本单位年度保密工作计划，报保密管理办公室备案后，按计划组织开展保密培训、检查等例行保密工作以及有关专项保密工作。年度保密培训计划与保密检查计划可以另行制订，也可以包含在年度保密工作计划中。

每年年底，保密管理办公室应当组织各单位上报年度保密工作总结，在此基础上，结合学校年度保密工作计划完成情况、日常保密管理情况以及保密监督检查情况，形成学校年度保密工作总结，除报告一年来保密工作开展情况，还应当对本单位的保密风险进行识别和分析，提出改进保密工作的意见建议，提交保密委员会审议，为确定下一年的保密工作重点提供决策参考。

（二）基层保密组织机构

高校具体承担涉密科研任务的单位是院系，密源在基层。因此，院系科研保密管理情况将直接影响和反映高校的整体管理水平。按照“分级管理，分级负责”的原则，高校在学校层面设立校保密委员会的同时，二级院系一般还要设立保密工作领导小组，特别是承担武器装备科研生产任务的院系。各涉密二级单位保密工作领导小组负责统筹协调本单位保密工作。其主要职责包括以下内容。

（1）研究、部署、落实学校各项保密工作要求和工作部署，解决存在的问题。

（2）组织制定本单位保密管理规章制度等。

（3）组织开展本单位保密宣传和保密教育培训。

（4）组织落实本单位涉密人员、涉密载体、涉密信息设备和存储介质的保密管理。

（5）协调保障本单位保密防护设备设施的建设与管理。

（6）组织涉密会议、涉外活动、新闻宣传等相关工作的保密审查和审批。

（7）组织开展本单位保密检查，并监督整改落实情况。

（8）配合调查失泄密事件及相关违规违纪行为。

（9）监督检查本单位保密责任制落实情况，组织实施本单位保密工作考核。

按照“业务工作谁主管，保密工作谁负责”的原则，院系保密工作领导小组一般由院系主要负责人或分管领导任组长，具体负责科研、党务、人事、教务、信息化的院系管理人员为组员，协助组长组织落实主管业务的保密工作，组成及分工参见表2-2。为了将院系保密管理工作责任层层分解，落实到人，按照要求，具体承担国防科研项目的基层单位（如研究所、实验室、课题组、项目组等）需配备兼职保密员，配合院系保密工作领导小组落实课题组的保密管理工作。按照《武器装备科研生产单位保密资格标准》要求，对一级保密资格单位，涉密人员数量100人以上的部门（院系或课题

组)，还应该配备 1 名专职保密工作人员。

表 2-2　高校基层单位保密领导小组构成示例

组成	岗　　位	主 要 职 责
组长	院系主要负责人或分管领导	全面负责院系保密工作
副组长	院系分管领导或保密要害部位负责人	协助组长履行保密管理职责
主要成员	院系科研管理人员（一般兼院系专兼职保密员）	院系涉密科研项目保密管理，院系级涉密集中场所保密管理
	院系教务管理人员	院系研究生及本科教学事务相关的涉密事项的管理
	院系人事党务管理人员	院系涉密人员的人事、党务审查
	院系机要文书管理人员	院系机要文件管理
	院系计算机、网络管理人员（一般兼计算机安全保密管理员）	院系信息系统与信息设备保密管理

为了保证(拟)承担涉密项目的院系具备开展保密工作的能力，切实发挥科研保密管理责任主体的作用，应当明确二级单位保密体系建设标准，包括组织机构、保密制度、保密场所防护设施等基本条件保障，经保密管理办公室验收达标后，方可开展涉密项目研究工作(参见附表 2-3)。

二、保 密 责 任

为了确保保密工作责任制落实，首先应当按照“业务工作谁主管，保密工作谁负责”和“分级管理、逐级负责”的原则，明确各级领导、相关人员的保密责任以及相关部门的保密工作管理职责与分工，其次是将保密工作责任制落实情况纳入学校各级领导班子及成员与相关人员以及相关部门的考核内容，并把考核结果与单位绩效、评奖评优及职务晋升等事项挂钩。

（一）各级领导和涉密人员保密责任

“保密责任”是武器装备科研生产单位保密资格审查认证评分标准的第一项。保密工作的顺利开展，离不开领导的重视，并在人、财、物等资源方面给予充分保障。学校主要负责人（校长或党委书记）对学校保密工作负全面领导责任，同样，各二级单位主要负责人对本单位保密工作负责。

1. 学校主要负责人（校长或党委书记）

作为学校保密工作第一责任人，对学校保密工作负全面领导责任，主要保密责任包括以下内容：

（1）将保密工作纳入学校党委重要议事日程，定期组织召开学校党委常委会议，研究解决学校保密工作中的重大问题。

（2）将中央关于保密工作的方针政策、党的保密纪律和保密法律法规列为学校党委理论学习中心组学习内容，并提出明确要求，带头贯彻执行。

（3）定期听取保密工作汇报，了解掌握保密工作情况，为保密工作开展提供人力、财力和物力等条件保障。

（4）重视发挥保密委员会职能，支持指导保密工作机构依法履行职责。

（5）监督学校保密工作责任制落实情况。

（6）其他应当履行的保密工作领导责任。

2. 分管保密工作校领导

对学校保密工作负具体领导责任，主要保密责任包括以下几项内容：

（1）及时组织传达、学习中央关于保密工作的方针政策、党的保密纪律和保密法律法规，部署贯彻实施和监督检查。

（2）组织制定并实施保密规章制度和工作计划。

（3）组织召开保密委员会会议，组织研究并协调解决保密工作中的重点、难点问题，向学校党委报告保密工作开展情况，将保密工作重大事项提交学校党委常委会议研究，组织落实学校党委关于保密工作的决定。

（4）组织开展保密宣传教育、保密检查、保密技术防护、失泄密事件查处和考核表彰等工作。

（5）监督检查学校保密工作落实情况，并为保密工作机构履行职责提供保障。

（6）其他应当履行的保密工作领导责任。

3. 分管其他业务工作校领导

对分管工作范围内的保密工作负直接领导责任，主要保密责任包括以下内容：

（1）熟悉分管业务工作中的保密要求，将保密管理要求融入分管业务工作。

（2）组织制定分管业务范围内的保密管理制度。

（3）部署分管业务工作中的保密工作，并督促检查落实。

（4）在分管业务范围内为保密工作开展提供保障。

（5）其他应当履行的保密工作领导责任。

4. 学校所属各单位（院系所、部处）主要负责人

作为本单位保密工作责任人，对本单位保密工作负直接管理责任。

（1）熟悉本单位保密工作整体情况，及时研究解决本单位保密工作重要问题。

（2）明确本单位人员的岗位保密职责，按照工作需要控制国家秘密的知悉范围。

（3）将保密管理要求融入日常工作中。

（4）定期开展保密教育和监督检查，采取具体措施组织落实学校保密工作部署。

（5）为本单位保密工作开展提供支持和保障。

5. 涉密科研项目、课题组负责人

作为本科研项目、课题组的保密工作责任人，对本科研项目、课题组的保密工作承担直接管理责任。

（1）直接掌握和管理项目保密工作，认真落实保密法律法规、规章制度，确保涉密项目全过程符合保密要求。

（2）做好项目产生的国家秘密的密级、保密期限和知悉范围的拟定工作，严格按照工作需要控制国家秘密的知悉范围。

（3）明确项目组成员保密职责，组织学习保密法律法规、规章制度及保密知识，提高保密意识和技能。

（4）严格管理项目组涉密载体，并明确专人负责，确保涉密载体安全。

（5）加强项目组信息设备和存储设备的保密管理，配备必要的安全保密设备。

（6）监督检查项目组保密工作落实情况，及时组织整改。

6. 涉密人员

学校每个涉密人员对本岗位保密工作负直接责任。

（1）认真学习并严格遵守保密法律法规、规章制度。

（2）了解岗位工作中国家秘密事项的情况及保密工作重点，熟悉本岗位保密职责。

（3）按要求参加保密教育培训，熟练掌握基本的保密知识和技能，认真履行岗位保密职责。

（4）接受学校和所在单位的保密监督检查，对检查发现的问题及时整改落实。

（5）发现失泄密隐患和失泄密情况及时报告，主动制止违法违规行为。

7. 涉密学生指导教师

作为研究生保密管理的第一责任人，对学生的保密工作承担直接管理责任。

（1）严格按照工作需要确定并控制知悉国家秘密的研究生范围，提出具体保密要求，进行保密教育和提醒。

（2）直接负责涉密研究生使用信息设备和存储设备、涉密载体的保密管理工作。

（3）负责涉密研究生发表论文、合作研究、技术交流、毕业论文等的保密审查。

（4）监督检查涉密研究生保密工作情况，及时督促整改。

（二）归口管理与相关部处保密工作主要职责

科研保密管理工作不仅覆盖科研项目研制全过程，还与涉密人员、科

研场所、科研设备与载体、科研档案、科研经费管理等各方面工作息息相关。学校应当根据涉密业务属性，结合高校内设部门机构职能，按照“业务工作谁主管，保密工作谁负责”的原则，合理确定各项业务归口管理部门。各归口管理部门在学校保密委员会领导和保密工作机构指导下，负责制定业务工作范围内的相关保密制度和工作制度，并将相关保密要求融入业务工作流程中，确保涉密业务开展到哪里，保密要求延伸到哪里，促进业务工作与保密工作的相互融合发展。

根据业务分工，学校相关部处保密职责参考如下。

1. 党委办公室

党委办公室负责学校机要文件的归口管理，主要职责包括以下内容：

（1）组织制（拟）定并实施学校机要文件管理规章制度。

（2）在学校授权范围内组织开展党政事务相关定密工作。

（3）协助校领导做好日常保密工作。

2. 科技处

科技处负责学校涉密项目的归口管理，主要职责包括以下内容：

（1）组织制（拟）定学校科研保密管理规章制度。

（2）组织开展学校科研项目等相关定密工作。

（3）负责与科研项目相关的保密审查工作。

（4）负责涉密科研项目管理过程中的保密工作。

3. 人事处

人事处负责涉密人员的归口管理，主要职责包括以下内容：

（1）组织制（拟）定学校涉密人员管理规章制度。

（2）负责涉密人员上岗、在岗、离岗管理以及涉密人员信息的管理。

（3）负责向公安机关出入境管理部门登记备案涉密人员变动情况。

（4）负责涉密人员因私出国（境）相关管理工作及证件管理。

（5）组织实施涉密人员保密教育培训，组织新入职人员的保密宣传教育。

（6）发放涉密人员保密补贴。

（7）组织涉密人员年度考核。

4. 信息化管理部门

信息化管理部门负责学校信息系统、信息设备、存储设备的安全保密归口管理，主要职责包括以下内容：

（1）组织制（拟）定信息化安全保密管理规章制度。

（2）监管信息化运维部门运行维护过程中的保密管理工作，落实安全保密检查。

（3）负责组织学校信息设备、存储设备的台账管理、安全审计和失泄密风险自评估工作，并监督整改落实。

5. 信息化运维部门

信息化运维部门保密工作主要职责包括以下内容：

（1）负责落实互联网信息安全保密管理要求和监管措施。

（2）负责涉密信息系统、信息设备、存储设备的运行维护，制定相关工作规范，建立工作档案，落实安全保密要求。

（3）负责落实学校信息设备、存储设备的安全审计、失泄密风险自评估工作，并及时整改落实。

（4）为调查失泄密事件及相关违规违纪行为提供信息化技术支持。

6. 宣传部

宣传部负责学校新闻宣传保密工作的归口管理，主要职责包括以下内容：

（1）组织制（拟）定新闻宣传保密管理规章制度。

（2）开展全校保密普法宣传教育。

（3）审批涉及涉密单位和涉密人员的采访申请。

（4）对相关宣传活动进行保密审查。

7. 研究生院

研究生院保密管理工作主要职责包括以下内容：

（1）负责涉密研究生上岗、在岗、离岗、离校管理以及涉密研究生信息的管理。

（2）负责研究生涉密学位论文作者的培养过程管理。

（3）负责研究生招生考试考务保密管理工作。

8．国际处

国际交流合作处（港澳台办公室）负责学校涉外活动保密工作的归口管理，主要职责包括以下内容：

（1）负责涉密人员因公出国（境）相关管理工作及证件管理。

（2）负责外事接待与交流等涉外活动的保密管理工作。

9．保卫处

保卫处保密管理工作主要职责包括以下内容：

（1）负责重要涉密、涉外活动的安全保卫工作。

（2）负责涉及国家安全的相关保密管理工作。

（3）负责指导、检查、监督保密要害部门部位防护设备设施的建设与管理。

（4）配合涉密人员资格审查进行必要的国家安全背景调查。

10．组织部

组织部负责干部保密责任制落实情况年度考核工作。

11．纪委办公室监察室

纪委办公室（监察室）负责对保密违法违规或泄密事件中涉嫌违反党纪党规行为进行调查，对有关责任人进行党纪处理。

12．档案馆

档案馆负责管理入馆涉密档案，对各单位保密档案管理工作进行业务指导和培训。

13．设备处

设备处负责涉密项目设备购置等的保密管理工作。

14．财务处

财务处负责学校涉密项目的经费管理，配合上级机关、相关单位进行涉密项目审计工作。

（三）保密责任书

为了强化保密责任，推动保密责任制落实，很多高校结合不同岗位，组织层层签订保密责任书，把保密责任分解到每个人。同时，将各级领导与各类涉密人员保密责任履职情况纳入年度考核内容。

1. 与学校主要负责人/保密委主任签订保密责任书

（1）各院系（所）、部（处）主要领导与学校主要负责人签订保密责任书；

（2）保密委成员（含副主任）与保密委主任签订保密责任书；

（3）各院系保密工作领导小组组长与保密委主任签订保密责任书。

2. 与各院系保密工作领导小组组长/保密委员会委员签订保密责任书

（1）各院系保密工作领导小组成员与组长签订保密责任书；

（2）各院系项目负责人与保密工作领导小组组长签订保密责任书；

（3）各机关部处专兼职保密员、涉密管理岗位人员与本单位保密工作领导小组组长或保密委员会委员签订保密责任书。

3. 与项目负责人签订保密责任书

（1）参与项目科研及管理工作的涉密人员与项目负责人签订保密责任书；

（2）项目组的非涉密人员与项目负责人签订保密责任书。

4. 涉密学生与导师签订保密责任书

责任书主要包括两部分内容：岗位保密责任及保密承诺，常用保密责任书范本参见附件 2-4～附件 2-14。

附件 2-1　保密委员会工作规则框架

＊＊大学保密委员会工作规则（框架）

为了保障学校保密工作顺利开展，进一步规范保密委员会工作程序，依据《＊＊大学保密工作责任制实施办法》，结合我校实际，制定本规则。

一、主要职能

学校保密委员会负责统筹协调全校保密工作，主要职责为：＊＊＊

保密管理办公室作为学校保密委员会下设日常工作机构，负责组织协调、指导、监督、检查各单位保密工作。

二、组成与调整

1. 成员组成

主任、副主任委员：

委员：

办公室主任：保密管理办公室主任兼任

2. 成员调整程序

三、会议组织

1. 会议形式

年度例会

专题会议

2. 列席人员

根据工作需要，相关部门具体工作人员可列席参加并汇报工作。

四、决策与工作落实

五、工作审批

六、考核与评优

- 责任
- 考核
- 评优

本规则自发布之日起施行。

附件 2-2　年度保密工作计划示例

＊＊大学＊＊年度保密工作计划

一、2 月，起草年度工作要点与计划

（一）起草《＊＊大学＊＊年度保密工作要点》；

（二）制订《＊＊大学＊＊年度保密宣传教育培训工作计划》；

（三）制订《＊＊大学＊＊年度保密检查工作计划》；

二、3 月，组织召开保密委员会全体会议

（一）传达上级有关文件精神；

（二）汇报《＊＊大学＊＊年度保密工作要点》与工作计划；

（三）审议相关规章制度；

（四）审议有关重要工作。

三、4 月，组织春季学期全校保密工作例行检查

四、5 月，组织到兄弟院校调研学习

五、10 月，组织秋季学期全校保密工作例行检查

六、11 月，组织到兄弟院校调研学习

七、12 月，组织保密委员会全体会议

（一）传达上级有关文件精神；

（二）审议年度保密先进集体和个人评选结果；

（三）审议相关规章制度；

（四）汇报保密管理工作情况与秋季学期保密检查情况；

（五）本年度保密管理工作总结；

八、其他工作

（一）3 月、6 月、9 月、12 月中下旬，组织 4 次涉密载体销毁；

（二）组织保密宣传教育培训，具体见专项工作计划；

（三）组织开展其他专项工作。

附表 2-3　二级单位保密体系审批表示例

＊＊大学所属二级单位保密体系审批表

<table>
<tr><td>单位名称</td><td colspan="2"></td><td>办公地点</td><td></td></tr>
<tr><td>建立保密体系原因</td><td colspan="4"></td></tr>
<tr><td rowspan="5">保密工作领导小组构成</td><td>姓　名</td><td>职务/岗位</td><td colspan="2">主 要 职 责</td></tr>
<tr><td></td><td></td><td colspan="2"></td></tr>
<tr><td></td><td></td><td colspan="2"></td></tr>
<tr><td></td><td></td><td colspan="2"></td></tr>
<tr><td></td><td></td><td colspan="2"></td></tr>
<tr><td>保密制度情况</td><td colspan="4"></td></tr>
<tr><td>涉密场所防护建设情况</td><td colspan="4"></td></tr>
<tr><td>单位保密承诺</td><td colspan="4">负责人签字：
（盖章）
年　月　日</td></tr>
<tr><td>保密管理办公室审核意见</td><td colspan="4">负责人签字：
（盖章）
年　月　日</td></tr>
<tr><td>保密委员会审定意见</td><td colspan="4">负责人签字：
（盖章）
年　月　日</td></tr>
</table>

附件 2-4　院系(所)、部(处)主要领导保密责任书示例

院系(所)、部(处)主要领导保密责任书

一、保密工作责任

(一)对本单位的保密工作负全面领导责任;

(二)及时传达学校有关保密工作要求,并采取措施进行部署和落实;

(三)掌握本单位的保密工作情况,研究解决本单位保密工作问题;

(四)对本单位的保密工作责任制落实情况进行监督和检查;

(五)为保密工作提供必要的条件支持和保障。

二、作为本单位保密工作主要负责人,我郑重承诺:

(一)认真遵守国家保密法律、法规和规章制度,履行保密义务;

(二)全面配合学校各项保密规章制度和管理措施,做好本单位保密工作。

单　　位:

主要负责人:　　　　　　　　**学校主要负责人:**

年　　月　　日　　　　　　　　**年　　月　　日**

附件 2-5　保密委员会副主任保密责任书示例

保密委员会副主任保密责任书

一、保密工作责任

（一）对分管工作范围内的保密工作负领导责任；

（二）对分管工作中的保密工作进行研究和部署；

（三）对分管工作中保密措施落实情况进行监督检查；

（四）为分管工作中的保密工作开展提供保障。

二、作为学校其他保密工作负责人，我郑重承诺：

（一）认真遵守国家保密法律、法规和规章制度，履行保密义务；

（二）认真抓好分管工作范围内的保密工作，不断完善学校保密工作长效机制。

责任人：　　　　　　　　　　**校保密委员会主任：**

年　　月　　日　　　　　　　　　　**年　　月　　日**

附件 2-6　保密委员会委员保密责任书示例

保密委员会委员保密责任书

一、保密工作责任

（一）对本单位业务范围内的保密工作负领导责任；

（二）及时传达学校有关保密工作要求，并采取措施进行部署和落实；

（三）掌握本单位业务范围内的保密工作情况，研究解决本单位业务范围内保密工作问题；

（四）对本单位业务范围内的保密工作落实情况进行监督和检查；

（五）组织和落实本单位涉密人员的年度保密考核；

（六）积极开展对本单位涉密人员的教育培训；

（七）为保密工作提供必要的条件支持和保障。

二、作为本单位保密工作负责人，我郑重承诺：

（一）认真遵守国家保密法律、法规和规章制度，履行保密义务；

（二）全面配合学校各项保密规章制度和管理措施，做好本单位业务范围内保密工作。

单　位：

责任人：　　　　　　　　　　**校保密委员会主任：**

年　　月　　日　　　　　　　　**年　　月　　日**

附件 2-7　院系保密工作领导小组组长保密责任书示例

院系保密工作领导小组组长保密责任书

一、保密工作责任

（一）对本单位的保密工作负直接领导责任；

（二）及时传达学校有关保密工作要求，并采取措施进行部署和落实；

（三）掌握本单位的保密工作情况，研究解决本单位保密工作问题；

（四）每季度对本单位的保密工作落实情况进行监督和检查；

（五）每季度组织开展对本单位涉密人员的教育培训；

（六）组织和落实本单位涉密人员的年度保密考核；

（七）配合学校保密部门对泄密事件的查处。

二、作为本单位保密工作主管领导，我郑重承诺：

（一）认真遵守国家保密法律、法规和规章制度，履行保密义务；

（二）全面配合学校各项保密规章制度和管理措施，做好本单位保密工作。

单　位：

责任人：　　　　　　　　**校保密委员会主任：**

年　　月　　日　　　　　　　　**年　　月　　日**

附件 2-8　保密管理人员保密责任书示例

保密管理人员保密责任书

一、保密工作责任

(一)学习领会上级保密工作精神和学校保密工作要求,并负责向本单位汇报、传达;

(二)接受学校保密管理部门的指导、监督和检查,并协助开展各项保密工作;

(三)协助本单位主管保密工作领导开展日常保密管理工作,监督、检查保密制度在本单位的执行情况;

(四)准确掌握本单位保密管理基础数据,并分类建立、及时更新台账,进行动态管理;

(五)及时向本单位主管领导和学校保密管理部门反映本单位保密工作存在的问题,并积极配合整改工作;

(六)完成本单位领导及学校保密管理部门安排的其他保密工作任务。

二、作为学校保密管理人员,我郑重承诺:

我清楚自身保密职责,认真履行保密责任,保护国家秘密安全,如因个人原因造成泄密,愿承担由此引起的一切后果。

单　位:

责任人:　　　　　　　　　　**单位主管领导:**

年　　月　　日　　　　　　　　**年　　月　　日**

附件 2-9　计算机安全保密管理员保密责任书示例

计算机安全保密管理员保密责任书

一、保密工作责任

（一）负责本单位涉密人员计算机的日常保密管理工作；

（二）配合学校计算机保密管理工作小组，组织实施计算机及信息系统安全保密检查；

（三）建立、更新、维护涉密计算机、涉密移动存储介质、通信及办公自动化设备等台账；

（四）办理涉密计算机的审定、调整、变更及涉密便携式计算机携带外出等手续，审核本单位计算机及信息系统的变更、维修、报废、软件安装等申请；

（五）定期升级涉密计算机防病毒软件，及时安装涉密计算机的操作系统、数据库和应用系统的补丁程序；

（六）完成本单位领导及学校保密管理部门安排的其他计算机信息系统及通信、办公自动化设备的保密工作任务。

二、作为学校计算机安全保密管理员，我郑重承诺：

我清楚自身保密职责，认真履行保密责任，保护国家秘密安全，如因个人原因造成泄密，愿承担由此引起的一切后果。

单　位：

责任人：　　　　　　　　　　　**单位主管领导：**

年　　月　　日　　　　　　　　**年　　月　　日**

附件 2-10　涉密管理人员保密责任书示例

涉密管理人员保密责任书

一、保密工作责任

（一）遵守国家保密法律法规和学校的各项保密规章制度；

（二）清楚本职岗位保密事项和保密要求；

（三）按规定履行保密工作职责；

（四）每年接受保密教育的时间达到规定要求；

（五）每月进行 1 次保密自查，积极配合学校和各单位组织的保密检查；

（六）熟悉保密应知应会和基本操作技能。

二、作为学校涉密人员，我郑重承诺：

我清楚自身保密职责，认真履行保密责任，保护国家秘密安全，如因个人原因造成泄密，愿承担由此引起的一切后果。

单　位：

责任人：　　　　　　　　　　**单位主管领导：**

年　　月　　日　　　　　　　　**年　　月　　日**

附件 2-11　课题（项目）组负责人保密责任书示例

课题（项目）组负责人保密责任书

一、保密工作责任

（一）对课题（项目）组保密工作负直接领导责任；

（二）掌握本课题（项目）组保密工作情况；

（三）采取具体措施组织落实单位保密工作部署；

（四）对本课题（项目）组保密工作提供支持和保障；

（五）指定专人负责本课题（项目）组保密管理，明确具体责任；

（六）对参加涉密项目研究的学生按要求做好保密教育和管理；

（七）对本课题（项目）组定期进行保密检查，发现问题及时整改。

二、作为课题（项目）组保密工作负责人，我郑重承诺：

（一）认真遵守国家保密法律、法规和规章制度，履行保密义务；

（二）对课题组参研人员做好保密教育，确保涉密项目研制全过程符合保密要求；

（三）全面执行学校、院系各项保密规章制度和管理措施，做好本课题（项目）组保密工作。

单　位：

责任人：	**院系主管领导：**
年　　月　　日	**年　　月　　日**

附件 2-12　课题组涉密人员保密责任书示例

课题组涉密人员保密责任书

一、保密工作责任

（一）遵守国家保密法律法规和学校的各项保密规章制度；

（二）清楚本职岗位保密事项和保密要求；

（三）按规定履行保密工作职责；

（四）每年接受保密教育的时间达到规定要求；

（五）定期进行保密自查，积极配合学校和各单位组织的保密检查；

（六）熟悉保密应知应会和基本操作技能。

二、作为学校涉密人员，我郑重承诺：

我清楚自身保密职责，认真履行保密责任，保护国家秘密安全，如因个人原因造成泄密，愿承担由此引起的一切后果。

单　位：　　　　　　　　**课题组：**

责任人：　　　　　　　　**课题组负责人：**

年　　月　　日　　　　　　**年　　月　　日**

附件 2-13　涉密课题组非密人员保密责任书示例

涉密课题组非密人员保密承诺书

我了解有关保密法规制度，知悉应当承担的保密义务和法律责任。本人庄重承诺：

一、认真遵守国家保密法律、法规和学校保密规章制度，履行保密义务；

二、遵守涉密场所保密管理规定，不该看的不看、不该听的不听、不该说的不说；

三、不提供虚假个人信息，自愿接受保密审查和保密教育；

四、不违法违规记录、存储、复制、留存国家秘密信息和秘密载体。

违反上述承诺，自愿承担党纪、政纪责任和法律责任。

承诺人签名：

年　　月　　日

附件 2-14　军工专家保密责任书示例

军口专家保密承诺书

我因工作需要，作为军口专家参加国防项目评审，了解有关保密法规制度，知悉应当承担的保密义务和法律责任。本人庄重承诺：

一、认真遵守国家保密法律、法规和学校保密规章制度，履行保密义务；

二、严格遵守会议组织方的保密管理要求，不违规记录、存储、复制、留存国家秘密信息和秘密载体；

三、不以任何方式泄露所接触和知悉的国家秘密；

四、不擅自发表涉及未公开工作内容的文章、著述。

违反上述承诺，自愿承担党纪、政纪责任和法律责任。

承诺人签名：

单位：

年　　月　　日

第三章　科研保密管理制度建设

科研保密管理制度是高校开展科研保密工作的依据，建立健全完善的保密管理制度是做好保密工作的基础。保密管理制度建设的关键是在符合国家法律法规的基础上，尽可能符合学校实际情况，增强可操作性。

一、科研保密管理制度体系

高校科研保密管理制度一般包括综合制度、基本制度、专项制度、业务制度，各所属院系根据学科特点和工作需要还可制定二级制度。一般来说，综合制度、基本制度、业务制度适用范围均为面向全校，分别针对高校整体、某一要素（如涉密载体）/某一环节（如涉密会议），或某一业务类型（如科研项目、学位论文）制定，而专项制度与二级制度仅适用于特定工程（如重点型号），或特定部门/对象（对涉密复印室）。

（一）综合制度

保密工作综合制度也是学校管理制度体系的基本制度之一，描述单位保密管理基本轮廓与总体要求，也为制定保密工作基本制度、专项制度等提供框架，主要内容一般包括总则、保密组织机构与职责、保密范围、管理要求、监督检查与奖惩、附则等部分。

“总则”部分明确学校保密工作的宗旨、适用范围、保密工作的方针与原则；“保密组织机构与职责”部分明确学校的保密管理组织体系与保密工

作责任制度；“保密范围”部分规定保密工作管理的对象；“管理要求”部分对定密、涉密人员、涉密载体、涉密计算机、涉外活动、涉密会议等保密管理主要要素作出原则性规定；“监督检查与奖惩”部分对保密工作的检查、责任追究与奖惩等作出规定；“附则”部分明确实施时间及解释部门。参考范本见附件 3-1。

（二）基本制度

基本制度是针对单位保密工作某一环节或某一要素的制度规范。根据《武器装备科研生产单位保密资格标准》要求，承担国防科研任务的高校必须建立包括保密责任（含归口管理责任）、定密工作、涉密人员、保密教育培训、国家秘密载体、密品、保密要害部门部位、信息系统、信息设备和存储设备、新闻宣传、涉密会议、协作配套、涉外活动、外场试验、保密监督检查、泄密事件报告和查处、考核与奖惩等 18 方面的基本保密制度，基本涵盖了学校科研保密工作各个方面。具体基本制度的数量及名称可以根据各个学校的习惯做出个性化规定，但内容应覆盖以上 16 方面的基本要求。如保密教育培训管理办法可以与涉密人员管理办法分别制定，也可以作为涉密人员管理办法的一个章节；信息系统、信息设备和存储设备可以作为一个基本制度，也可以根据各高校的工作习惯分为计算机和存储设备保密管理办法、通信及办公自动化设备保密管理办法等两项制度，甚至每类设备也可以针对涉密、非涉密两种情况分别制定保密管理办法。

（三）专项制度

专项制度是任务承担部门针对某项重大工程/重点型号制定的专项保密管理措施。由于重大涉密工程或涉密项目具有涉密程度高、研制周期长、外协单位多等特点，按照《武器装备科研生产单位保密资格标准》，要求对所承担的每一项重大涉密工程或项目都要制定一项专项制度。专项制度应当根据项目特点和任务要求，对任务实施的各个阶段和各个环节，明确责任部门与具体的管理措施，经保密管理办公室审议通过后施行。

（四）业务制度

业务制度是单位业务主管部门针对某项业务而制定的保密管理制度。如《涉密科研项目保密管理办法》《研究生学位论文保密管理办法》《涉密设备采购与管理保密实施办法》《涉密项目科研经费保密管理办法》和《涉密地质资料使用保密管理办法》等。一般应由单位业务主管部门在保密管理办公室指导下制定，按照业务流程，把保密管理基本制度的要求融入业务工作中。

（五）二级制度

二级制度是由单位内部的涉密部门（单位）为了更好地贯彻学校保密管理要求，依据学校基本制度，结合本单位保密工作职能分工与业务工作实际，制定的具体保密管理措施，既包括适用于本部门（单位）的综合性制度，如《院系保密管理实施细则》，也包括针对某一场所或管理对象的专门的保密管理办法，如《涉密复印室保密管理办法》《保密资料室保密管理办法》《涉密场所（机房、实验室等）保密管理办法》，等等。

高校保密管理制度应自成体系，满足“符合性、完整性、一致性、可操作性”等要求。符合性是指与上位法相符合，既包括学校综合性制度与国家、行业保密法律法规一致，也包括学校的专项制度、二级制度符合学校综合性制度、基本制度规定；完整性是指要涵盖学校保密工作各个方面的需要，从科研保密需要出发，应涵盖《武器装备科研生产单位保密资格标准》规定的各要素；一致性是指制度之间相互衔接配套，不能相互矛盾；可操作性则是为了便于制度落实，应确保规定具体、责任明确、流程清楚、配套表格完备。

如表 3-1 所示的制度清单中所列的制度基本上能够满足学校科研保密工作需要，并且符合《武器装备科研生产单位保密资格标准》要求。

为了方便使用，高校一般把适用于全校的保密管理制度汇编成册，通常包括综合制度、基本制度与业务制度，经校长或党委书记签字后发布，参见附件 3-2 文件发布令。

表 3-1　高校科研保密管理制度清单

类　型	制度名称	说　　明
综合制度	保密工作管理规定	由校务会/党委常委会讨论通过
基本制度	保密工作责任制	由保密管理办公室组织制定，报学校保密委员会审议通过
	定密工作管理规定	
	涉密人员管理办法	
	保密宣传教育实施办法	
	国家秘密载体保密管理办法	
	密品保密管理办法	
	保密要害部门部位管理办法	
	信息系统、信息设备和存储设备保密管理办法	
	宣传报道保密管理办法	
	涉密会议管理办法	
	协作配套保密管理办法	
	涉外活动保密管理办法	
	外场试验保密管理办法	
	保密检查工作实施办法	
	泄密事件报告和查处管理办法	
	保密工作考核与奖惩管理办法	
专项制度	重大涉密项目/工程保密管理办法	任务承担部门根据工作需要制定，报学校保密管理办公室审议
业务制度	涉密科研项目保密管理办法	各业务主管部门根据工作需要制定，报学校保密委员会审议
	研究生学位论文保密管理办法	
二级制度	＊＊院系保密管理实施细则	各院系等基层单位根据工作需要制定，经本单位院务会/系务会审议
	涉密复印室保密管理办法	
	保密资料室保密管理办法	
	＊＊涉密场所（机房、实验室等）保密管理办法	
	……	

二、基本制度

基本制度应当尽量做到“完整、准确、适用、可行”，即制度完整，涵盖《武器装备科研生产单位保密资格标准》规定的 16 个方面；依据准确，条款规范；及时修订，适应保密事业与业务工作发展需要；操作性强，文字描述与流程、表格相结合。

基本制度主要包含以下各项内容。

（一）保密责任

明确保密责任是落实保密责任制的前提，应当包括两个层面：一是学校各级领导和各涉密岗位的保密责任，二是科技处、人事处、信息化部门、国际处、宣传部等各职能部门在业务工作范围内的保密责任。这样，既体现“业务工作谁主管，保密工作谁负责”的基本原则，促进保密工作与业务工作相融合，也是落实保密工作“归口管理”的基本要求。

（二）定密管理

定密工作是做好保密工作的基础，应当明确定密工作的原则和范围，规定单位定密责任人、承办人以及学校各级保密工作组织在定密工作中的职责与基本要求，以及开展定密工作的依据，产生的国家秘密事项定密、变更与解密的工作程序，变更、解除所管理的国家秘密事项的具体要求，国家秘密标志与变更、解密标识等。为强调定密工作的严肃性，还应当明确定密工作的法律责任。

（三）涉密人员管理

涉密人员管理是保密管理的核心，保密管理要求应当覆盖其岗前、在岗、离岗的全过程。主要包括进入涉密岗位前的资格审查、保密培训与密级界定，在岗期间的保密教育、因私出国（境）管理与保密补贴发放等，离开

涉密岗位前的载体交接及保密承诺,脱离涉密岗位后的脱密期管理。涉密人员在岗期间处理涉密载体、使用涉密设备以及接受保密教育、发表论文、参加涉密会议与涉外活动等关键要素和重要活动都有专门的基本制度予以规范,在涉密人员管理基本制度可作原则规定,简要加以描述。

(四)保密教育

接受保密教育是全校师生员工及相关人员应尽的义务。作为学校的保密教育制度,不仅要有针对涉密人员的专业培训要求,还应包含面向全校师生,以及干部、学生等特定人群的面上教育,应当明确各类培训的组织部门以及保密培训的形式、内容、工作程序、学时要求等。

(五)载体管理

涉密载体管理的基本要求是底数清楚,从“生”到“死”全程有记录、可追溯。载体管理基本制度应当包含涉密载体制作、收发、传递、借阅、使用、复制、保存、销毁等全过程的管理要求,明确需要审批、登记的环节。为了使载体管理过程受控,结合本学校的管理模式,应当对制作、复制、保存、销毁等环节实行相对集中管理,特别是复制、销毁环节,尽可能集中到学校层面;为了掌握学校涉密载体底数,对机关部处、院系、课题组的载体台账要求要做出规定,并保证追溯期限不少于3年。

同时,应当明确涉密载体管理和使用的“红线”,包括不得非法获取、持有涉密载体,不得非法复制、记录、存储国家秘密,不得买卖、转送或者私自销毁涉密载体,以及传递与寄带出境方面的“高压线”等内容。

(六)密品管理

针对密品的特殊性,最新的保密资格标准要求武器装备科研生产单位专门制定密品管理方面的基本制度,而不能把它作为涉密载体管理的一部分。除了需要明确对密品进行全生命周期管理的要求外,需重点强调其不同于涉密载体管理的方面。比如,关于标识以及存放方式,除了要按照国

家有关规定在密品上作出国家秘密标志，还要在有关技术文件中注明；对外形和构造容易暴露国家秘密的密品，在研制、生产、试验、运输、保存、维修、使用等过程中应当对其采取遮挡或其他保护措施等，重要密品运输过程还应当事先制定安全保密预案。

（七）要害部门部位管理

要害部门部位管理首先是尽可能集中，其次是准确界定，同时要对界定为要害部门部位的场所明确“人防、物防、技防”等防护措施建设标准，对要害部门部位的日常管理进行规范，比如非授权人员进出、工勤服务人员聘用及服务以及禁止带入电子设备（含手机）等提出明确要求。

（八）信息系统、信息设备和存储设备管理

由于信息系统、信息设备和存储设备管理业务性强，应当明确由单位信息化管理部门负责其安全保密管理，并指定或委托内部机构（单位）负责其运行维护。信息化大背景下，信息系统、信息设备和存储设备是失泄密的主要风险，也是各高校保密管理的重点和难点，应当对其全生命周期进行管控，包括投入使用前的审批、防护要求、访问权限控制、信息交互规范、运行维护要求以及退出涉密用途前技术处理等，还要明确红线，划清底线，包括直接带来泄密风险的行为，也包括破坏信息系统、信息设备和存储设备管理防护安全的行为以及逃避检查的行为等。

（九）新闻宣传管理

鉴于高校对外信息发布频繁，首先应当明确需保密审查审批的事项范围，其次规定保密审查审批的流程，包括责任部门。依据保密资格标准要求，涉及武器装备科研生产事项的宣传报道、展览、发表著作和论文等，应当经单位武器装备科研生产主管部门保密审查；涉及武器装备科研生产事项的参观、采访，应当履行审批手续，明确参观内容与路线、对外宣传口径；需报上级主管部门审批的，应当履行报批手续。

（十）涉密会议管理

对主办或承办的涉密会议，会前应确定会议密级，选择具备安全保密条件的场所与符合保密要求的音像等技术设备；针对重要的涉密会议，主办部门还应当制定保密方案；会中应当严格控制与会人员范围，指定专人负责涉密载体的发放、清退与保管，严禁带入手机等移动通信工具以及非主办方批准的拍摄、录音设备，必要时保密工作机构派人监督和检查。

（十一）外场试验管理

外场试验通常多个单位共同参与，其保密管理工作由牵头单位负责组织协调，各参试单位明确保密负责人予以配合。管理内容包括外场试验前制定保密工作方案，试验现场对各参试单位人员及涉密设备、通信、涉密载体和密品的管理进行监督检查，试验结束后的保密总结。

（十二）协作配套管理

主要包括合同签订前应当对涉密协作配套单位保密资格进行审查，合同不得涉及项目研制必需之外的涉密信息，保密条款或保密协议中应当明确界定合同文本和项目的密级、保密要求和保密责任，执行中监督检查协作配套单位保密管理要求落实情况等。对承接高校分包的《武器装备科研生产许可目录》之外的应急或者短期秘密级项目的协作配套单位，如尚未取得保密资格，学校应对其保密管理的基本条件和能力进行审查，并签订保密协议、提出保密要求，对其履行情况进行监管。

（十三）涉外管理

内容中应当规范对外合作、交流和谈判等涉外活动的范围、活动区域、介绍口径、对外提供资料保密审查等要求。一是明确管理的范围，包括本单位组织或参加对外交流、合作和谈判等外事活动，以及接待境外人员来

访等；二是明确管理的要点，组织或参加对外交流、合作和谈判等外事活动的责任部门，应当明确保密负责人，制定保密方案，明确保密事项，采取相应的保密措施，交流内容、谈判口径、提供资料和产品应当经过保密审查；接待境外来访人员，应当对其身份进行确认，明确活动区域，采取相应的安全保密防范措施；三是明确单位主管部门的监管职责，对上述外事活动，执行保密提醒制度，对接待境外人员来访，履行审批手续。

对涉及国家秘密的涉外活动，还应当报上级主管部门履行审批手续。

（十四）保密检查

一是规范检查的内容，如综合性检查或专项检查等；二是规范检查的方法，包括自查、互查和抽查等；三是规范检查的程序，包括检查周期、检查计划、检察队伍组织、检查中发现问题处理、检查后整改及验证等活动。

学校还应当根据日常管理和检查情况，结合保密检查情况分析报告或年度保密工作总结对单位存在的保密风险进行分析，提出改进措施，并督促落实。

（十五）泄密事件查处

一是发生泄密事件应当在规定的时间内向学校及上级主管部门及时报告；二是学校主管部门组织责任部门分析事件原因，并采取补救及整改措施；三是根据泄密事件危害评估结果，对有关责任人进行查处，并向上级主管部门报告查处情况。

（十六）考核与奖惩

主要应当明确考核与奖惩工作的组织、考核要求、奖励条件、惩处措施以及责任追究制度。要把学校各单位日常管理和检查情况与考核结果挂钩，把保密工作责任落实情况与绩效考核挂钩；要严格执行保密工作责任追究制度，除追究直接责任人的责任，还要追究相关领导的责任。

三、专项制度

专项制度是针对重点涉密工程或重大涉密项目专门制定的保密管理制度或保密工作方案，一般包括总则、职责分工、保密要点、管理措施、附则几部分章节，各部分主要内容参见表 3-2。保密专项制度范本参见附件 3-3。

表 3-2　专项制度主要内容

章	题　目	主 要 内 容
第一章	总则	依据、方针、原则、适用范围
第二章	职责分工	相关责任部门与分工
第三章	保密要点	项目涉密事项及密级、保密期限、知悉范围
第四章	管理措施	对项目所涉及涉密人员、设备、载体、场所、协作配套、外场试验等具体管理措施
第五章	附则	奖惩、解释部门

针对涉及的重要内容也可以形成单项制度，如＊＊任务外协人员管理办法、＊＊任务协作配套保密管理办法、＊＊任务涉密文件管理办法、＊＊任务外场试验管理办法等。

四、业务制度

业务制度是单位各业务主管部门为在业务工作中更好地贯彻学校保密管理的各项要求，根据各自的业务流程梳理出的各个阶段应当落实的保密工作，并明确保密管理部门与业务管理部门的工作接口，便于保密要求落地。一般包括总则、职责分工、各阶段/环节保密要点、附则几部分章节，各部分主要内容参见表 3-2。以《涉密科研项目保密管理办法》为例，保密业务制度范本参见附件 3-4。

五、二 级 制 度

二级制度作为对学校系统、完整的科研保密管理制度进一步的补充和细化，应充分结合具体部位或基层院系的实际情况，具有可操作性，可以是文字、表格、流程图等形式。如图 3-1 所示为高校某基层单位在学校保密规章制度基础上梳理的科研保密管理工作流程，图 3-2 为高校基层单位涉密资料复印、摘录/引用保密管理流程，既要条理清晰，又能一目了然，便于掌握和操作。本书选取涉密复印室管理方法作为一个典型案例，有关范本参见附件 3-5。

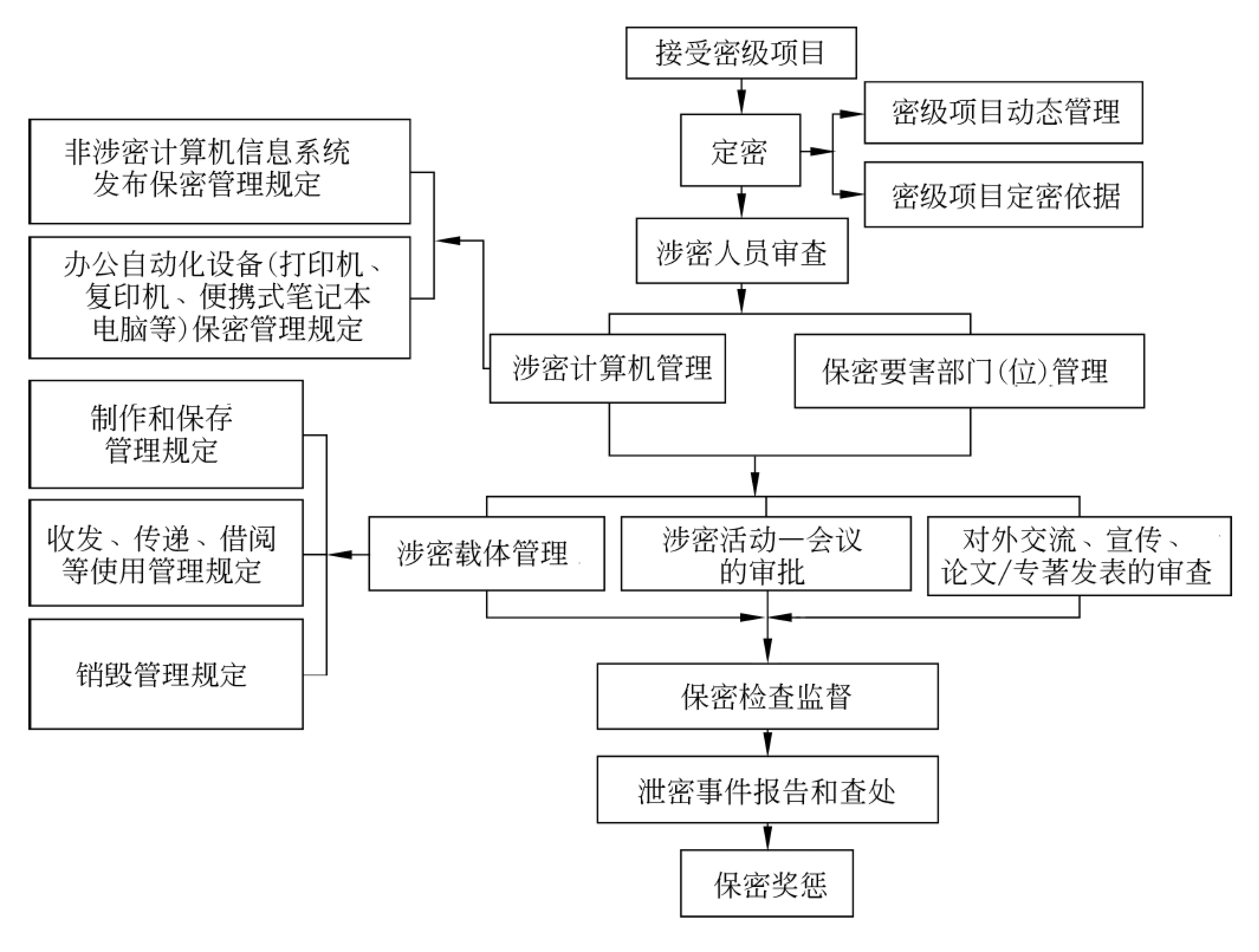


图 3-1　高校基层单位日常科研保密管理流程

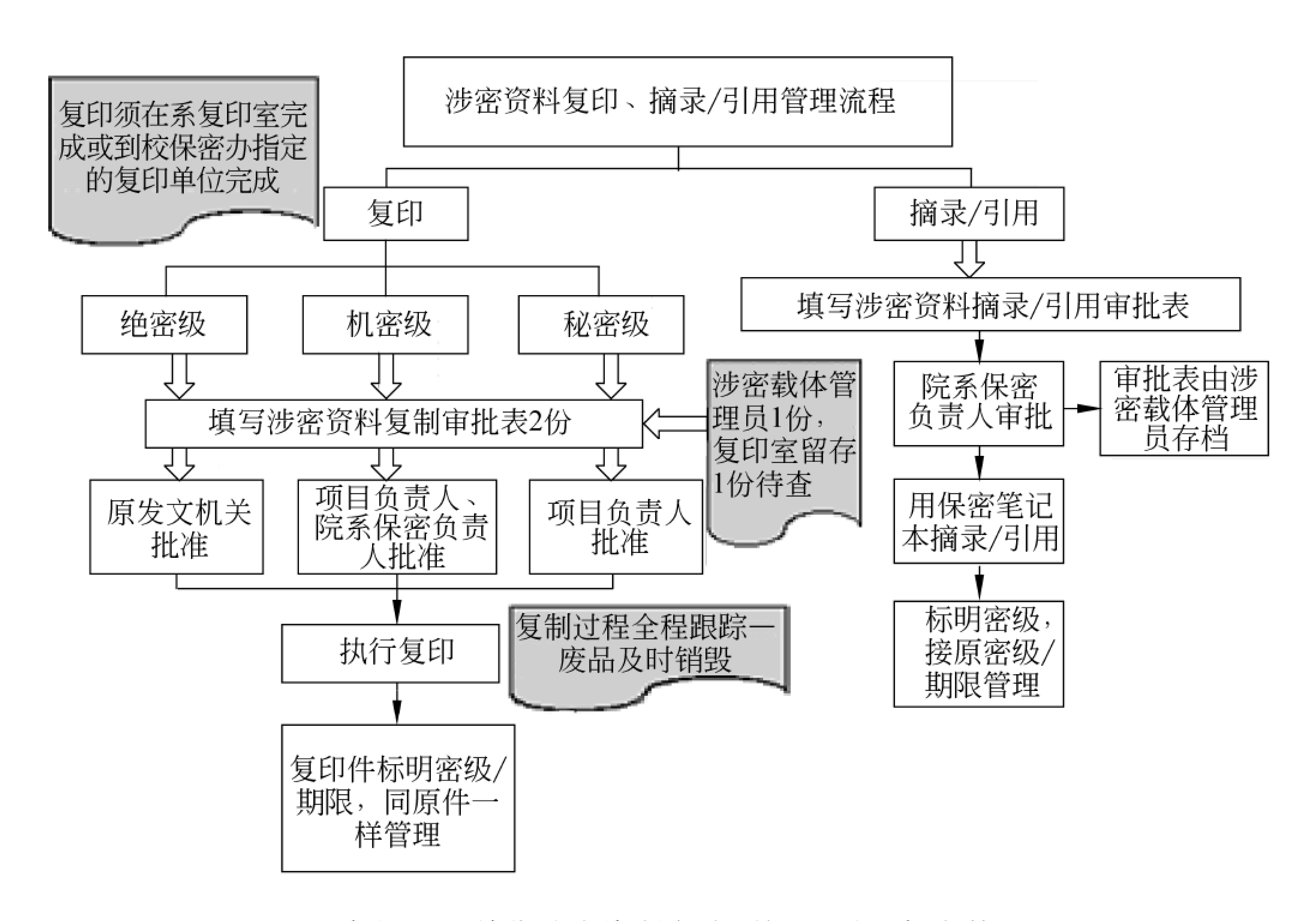


图 3-2　高校基层单位涉密资料复印、摘录/引用保密管理流程

附件 3-1　保密工作规定示例

＊＊大学保密工作规定

第一章　总　　则

第一条　为加强学校保密工作，根据《中华人民共和国保守国家秘密法》《中华人民共和国保守国家秘密法实施办法》及有关法律法规，结合本校实际情况，制定本规定。

第二条　本规定适用于学校所属各单位和全体师生员工。

第三条　保密工作贯彻“积极防范、突出重点、依法管理”的方针，既确保国家秘密安全，又便利信息资源合理利用。

第二章　保密组织机构与职责

第四条　学校实行三级保密工作管理体制。学校保密委员会负责全校的保密工作，下设保密管理办公室负责日常管理事务；学校所属各单位设立保密工作领导小组；涉及国家秘密的基层单位设保密管理人员，具体负责本单位保密工作。

第五条　保密管理责任制采取“业务谁主管，保密谁负责”和“分级管理、逐级负责”的原则。各级负责人须掌握分管业务的保密工作情况，切实履行保密工作职责；各单位保密工作领导小组须严格落实保密管理规章制度，负责部署、协调、督促和检查本单位保密工作；涉及国家秘密的基层单位须严格遵守相关保密管理规定，做好本单位保密工作。

第六条　学校校长/党委书记是学校法定定密责任人，对学校定密工作负总责。法定定密责任人根据工作需要授权学校相关业务主管部门负责人为指定定密责任人，负责主管业务的定密工作。

第三章　保 密 范 围

第七条　学校保密范围包括教学、科研、生产、公务活动中产生或承办的国家秘密和“内部事项”。国家秘密的密级分为“绝密”“机密”“秘密”三级。

不属于国家秘密，在一定时间内又不宜公开的事项，定为“内部事项”。

内部事项虽不属于国家秘密，但必须严格管理，未经批准，不得擅自扩散。

第四章　管理要求

第八条　[定密方面]产生国家秘密事项的单位，应及时根据定密的法定程序，指定承办人按相关规定报批。需对国家秘密事项的密级和保密期限变更时，应及时按原确定密级的程序办理。保密期限届满的，自行解密。

第九条　[人员方面]各级党政干部和所有涉密人员须接受保密教育。涉密人员须接受保密工作培训，并签署保密协议。涉密人员脱离涉密岗位时，应签订保密承诺书，实行脱密期管理。

涉密人员使用手机或具有存储传输等功能的电子产品，要严格遵守国家相关保密规定，不得在使用手机时涉及国家秘密事项。

第十条　[载体方面]制作、收发、传递、使用、复制、保存、维修和销毁国家秘密载体及其过程文件、资料，须遵守相关保密管理规定。国家秘密载体应标明密级和保密期限。

禁止非法复制、记录、存储国家秘密；禁止通过普通邮政等无保密措施的渠道传递国家秘密载体；禁止邮寄、托运国家秘密载体出境；禁止在私人交往和通信中涉及国家秘密。携带属于国家秘密的文件、资料和其他物品不得违反相关保密规定。

机要文件须由机要人员进行专门管理，机要文件的收发、传阅、保存、销毁应严格遵守相关保密管理规定。

第十一条　[设备方面]使用信息系统、信息设备和存储设备应遵守信息安全有关保密规定。禁止将涉密信息系统、涉密信息设备和涉密存储设备接入互联网和其他公共信息网络。禁止使用非涉密信息系统、非涉密信息设备和非涉密存储设备存储、处理、传输国家秘密信息。

第十二条　[场所方面]保密要害部门、部位须进行物理隔离，有完善有效的保密管理制度、符合规范要求的防护措施。

第十三条　[涉密会议]举办涉密会议时，主办/承办单位须依据有关规定提前制定保密方案，报学校保密管理办公室审批，并全程接受保密管理办公室的监督检查。

第十四条 [涉外活动]参加境内外的涉外活动,应遵守相关保密规定。不得携带涉密载体参加涉外活动。涉密人员出境须经报批。

第十五条 [宣传报道]拟宣传报道和出版发行的事项,须履行相关保密审查手续。涉及国家秘密的事项如确需在一定范围内进行宣传报道须统一宣传口径,并报经校保密管理办公室审查备案。

单位或个人如接受境内(外)机构、团体、个人及其委托的社会调查,不得涉及国家秘密或“内部事项”。

第十六条 [涉密项目]涉密项目(课题)组在申报立项、研制协作、论文和报告撰写、结题验收、资料归档、成果鉴定等过程中,须严格遵守相关保密管理规定。

第五章 监督检查与奖惩

第十七条 [监督检查]校保密管理办公室对各单位的保密工作进行指导、监督和检查。

第十八条 [泄密查处]发现国家秘密已经泄露或者存在泄密隐患时,应立即采取补救、保护措施,并及时报告,配合校保密管理办公室和上级有关部门进行查处。

第十九条 [考核与奖惩]各级党政干部和所有涉密人员保密工作履职情况纳入年度考核内容。学校对保守、保护国家秘密作出突出贡献以及在保密工作中取得显著成绩的单位和个人,给予表彰和奖励。对违反保密法律法规和本规定、故意或过失泄露国家秘密的,学校对相关责任人按规定给予相应处理。构成犯罪的,移交司法机关依法追究刑事责任。

第六章 附 则

第二十条 学校授权保密委员会依据本规定制定相应的管理办法或实施细则。

第二十一条 本规定由学校保密委员会负责解释。

第二十二条 本规定自公布之日起施行。

附件 3-2　文件发布令示例

文件发布令

自《中华人民共和国保守国家秘密法》及《中华人民共和国保守国家秘密法实施办法》实施以来,我校结合有关业务工作的具体情况,先后制定出一系列保密工作规章制度,有效地保障了我校教学、科研、生产与管理工作的顺利进行。

随着我校国防科研及人才培养工作的不断深入开展,为进一步规范我校保密管理工作,学校结合《武器装备科研生产单位保密资格认定办法》的要求,对原有规章制度进行补充、修订,并于 * * 年 * * 月 * * 日经校保密委员会讨论通过,其中,《保密工作管理规定》修订稿于 * * 年 * * 月 * * 日经 * * 学年度第 * * 次校务会议讨论通过。现将其汇集成册,予以发布,请遵照执行。

希望全校各级领导干部认真学习和掌握我校各项保密规章制度,从维护党和国家安全与利益的高度,带头执行和模范遵守各项保密法规与制度,积极向广大师生员工宣传教育,做好各自职权范围内的保密工作,真正使保密工作发挥“保安全、保发展”的重要作用,使我校保密工作再上一个新台阶。

校长/党委书记：

年　　月　　日

附件 3-3　* * 任务保密管理办法示例

* * 任务保密管理办法

第一章　总　　则

第一条　为保守“* * 任务”国家秘密，做好保密工作，杜绝失泄密事件发生，依据任务下达单位保密管理要求和学校保密管理规定，特制定本办法。

第二条　本任务保密工作遵循“积极防范、突出重点、依法管理”的方针，坚持“业务谁主管，保密谁负责”的原则，把保密工作与业务工作同部署、同检查、同奖惩，将保密管理融入任务执行过程的各个环节。

第三条　本办法适用于 * * 任务的各承研承制单位。

第二章　职责分工

第四条　本任务专门成立保密工作领导小组，组长由任务总指挥担任，副组长由总师担任，小组成员包括总师办主任与各分系统负责人。

第五条　本任务专门成立保密办，由总师办主任兼保密办主任，负责组织落实任务日常保密工作，根据需要制定专项（如协作配套、外场试验等）保密方案。

第三章　保密要点

第六条　本任务总体及各分系统涉密事项由任务总师依据学校定密程序组织各分系统负责人确定，同时确定各涉密事项的密级、保密期限、知悉范围，以及该任务包含的商业秘密、工作秘密。

第七条　任务总师及各分系统负责人应通过内部沟通后，确保知悉范围内人员掌握所参与工作的保密要点，并严格控制知悉范围。

第八条　任务总师应根据任务的进展情况，及时组织涉密事项的变更，包括及时调整知悉范围。

第四章　管理措施

第九条　人员管理（含内部涉密、非涉密人员及外协人员）。

第十条　设备管理（含涉密、非涉密设备，内部设备与外协单位设备）。

第十一条　密品、密件管理(含内部与外协单位的密品、密件管理)。

第十二条　涉密场所管理(含涉密复印室、资料室的管理以及接待参观、来访的管理等)。

第十三条　协作配套保密管理(含密级确定、保密协议及监督检查等)。

第十四条　涉密会议管理(含密级确定、会场及保障措施等)。

第十五条　外场试验管理(含密品运输,参试人员、设备、通信、密品密件的管理等)。

第五章　附　　则

第十六条　对在本任务保密管理工作中作出重大贡献的,或违反保密规定造成严重后果的,按照学校保密工作奖惩管理办法给予奖惩。

第十七条　本办法由任务总师办/保密办负责解释。

第十八条　本办法自公布之日起施行。

附件 3-4　涉密科研项目保密管理办法示例

涉密科研项目保密管理办法

第一章　总　　则

第一条　为进一步加强涉密科研项目保密管理，确保国家秘密的安全，根据《＊＊大学保密工作管理规定》及《＊＊大学国防科研项目管理办法》，结合学校实际，制定本办法。

第二条　本办法适用于学校承担的涉密国防科研项目的保密管理。涉密民口科研项目保密管理原则上遵照本办法执行。

第三条　涉密项目保密管理实行“业务工作谁主管，保密工作谁负责”和“分级管理、分级负责”的原则。

第二章　职　　责

第四条　项目负责人是涉密项目保密管理的第一责任人，按照保密工作与业务工作“五同时”（同计划、同部署、同检查、同总结、同奖惩）原则，直接负责组织落实所承担项目申报论证、立项、实施、验收和归档、鉴定报奖等全过程的保密管理工作。

第五条　各承担涉密项目的院（系、所）是其所承担项目的保密管理责任主体，负责组织、协调、监督、检查本单位涉密项目的保密工作，并为本单位开展涉密项目保密工作提供必要的组织保障和条件保障。

第六条　校科研管理部门是学校涉密项目的业务主管部门，负责组织开展与涉密项目相关的定密工作，协同校保密管理办公室完成与涉密项目相关的保密审查，组织指导相关院（系、所）在涉密项目全过程管理中贯彻本办法，并监督检查落实情况。

第七条　校档案馆是学校档案工作的业务主管部门，负责学校涉密项目档案的接收、整理、保管和利用等工作。

第八条　校财务处是学校财务工作的业务主管部门，负责学校涉密项目经费预决算的审核、审计接待及经费的管理。

第九条　校保密管理办公室是学校保密工作的业务主管部门，负责指

导、监督、检查涉密项目全过程的保密管理工作。

第三章　各阶段保密要点

第十条　建议与申报阶段保密要点(含人员涉密资格审查,保密提醒教育,保密条件保障,涉密载体管理等)。

第十一条　立项阶段保密要点(含项目涉密事项确定,开展涉密工作的人员、设备、工作场所条件审查等)。

第十二条　实施阶段保密要点(含校内分包、校外协作、涉密会议、对外交流、宣传报到,以及涉密事项变更等)。

第十三条　结题验收阶段保密要点(含资料归档、文件清理、人员、设备脱密等)。

第四章　重点环节保密要点

第十四条　成果鉴定或报奖保密要点(含申报国防成果保密条件保障与申报公开成果保密审查)。

第十五条　经费管理保密要点(涉及到款信息录入、项目财务名称命名、经费使用记录,以及经费决算与审计等环节)。

第五章　附　　则

第十六条　对在涉密科研项目保密管理工作中作出重大贡献的,或违反学校保密规定造成严重后果的,按照学校保密工作奖惩管理办法给予奖惩。

第十七条　本办法由校科研管理部门负责解释。

附件 3-5　涉密复印室管理规定示例

涉密复印室管理规定

本室为我校定点涉密复印室，为校内师生提供涉密文件的打印、刻录、复印、装订等服务，为加强服务过程的保密管理，特作如下规定。

一、本室涉密计算机、复印机由涉密复印员专人管理，凭“涉密资料复制审批表”提供服务，电子版文件使用我校专用涉密 U 盘传输；

二、凡委托复印或打印涉密资料（文件首页标明机密或秘密），委托人须出示“涉密资料复制审批表”，复印员认真检查审批表是否有审批人签字、所在院系主管部门盖章，确认手续齐备后方可提供服务；

三、复印员须认真核对打印、复印或装订页数与份数，确保按审批内容提供服务，打印或复印过程中产生的废纸废页应当场用碎纸机销毁；

四、打印、复印或装订过程中，委托人应全程在场，禁止无关人员接触；

五、本复印室涉密计算机不得存储涉密资料；

六、复制结束后，复印员将涉密资料全部交还委托人，不在复印室存留任何涉密资料（含纸质与电子版本）；

七、复制完成后，复印员在复制审批表上签字确认，并将审批表原件交给委托人，复印件按院系分类保存于保密柜中，并在《涉密材料复印登记表》上登记备案；

八、本复印室无权处理“绝密”级文件；

九、本办法自＊＊年＊＊月＊＊日实施。

第四章　涉密科研项目定密管理

涉密科研项目的定密，是指高校依据法律规定的定密权限、定密依据和定密程序，将学校在承担涉密科研生产任务过程中产生的关系国家安全和利益，在一定时间内只限一定范围内人员知悉的事项确定为国家秘密，以及对产生和管理的国家秘密进行变更和解密的活动。涉密科研项目的定密是涉密人员管理、国家秘密载体管理、涉密计算机与信息设备管理的基础，具有政策性、行业性、专业性，在整个科研保密管理中处于重要地位。

一、定密权限

学校应当根据定密权限依法开展定密工作。根据《国家秘密定密管理暂行规定》等文件规定，只有中央国家机关、省级机关以及设区的市、自治州一级的机关具有法定定密权，并可以对承担本机关定密权限内的涉密科研、生产或者其他涉密任务的机关、单位，就具体事项主动或者依申请作出定密授权。

因承担涉密科研、生产或者其他涉密任务，经常产生国家秘密事项、尚未取得定密授权或取得的定密权限满足不了实际工作需要的高校，可以向上级业务主管部门（如国防科工局）或上级机关（如教育部、工信部等）就具体事项申请相应密级的定密授权。近三年来，年均产生绝密级 6 件以上的单位可申请绝密级、机密级、秘密级定密权；年均产生机密级 6 件以上的单位可申请机密级、秘密级定密权；年均产生秘密级 6 件以上的单位可申请秘密级定密权。取得相应密级定密权限之前，有关定密工作可以报请具有

定密权限的上级业务主管部门或上级机关审批。取得定密授权的高校无权对其他不具备定密权限的单位再行授权。

仅仅执行上级机关、单位或者办理其他机关、单位已定密事项所产生国家秘密事项的高校，不需要申请定密授权。

二、定密责任人

针对定密工作中普遍存在的定密主体宽泛、责任不明确、程序不规范等问题，《中华人民共和国保密法》（以下简称《保密法》）专门设立了定密责任人制度。其中，第十二条规定："机关、单位负责人及其指定的人员为定密责任人，负责本机关、本单位的国家秘密确定、变更和解除工作。机关、单位确定、变更和解除本机关、本单位的国家秘密，应当由承办人提出具体意见，经定密责任人审核批准。"这就明确了定密的责任主体是定密责任人，只有经过定密责任人审批，国家秘密才能依法生成，具有法律效力。定密责任人又分为法定定密责任人和指定定密责任人两类人员。定密责任人应当接受定密培训，考核合格方能上岗。

（一）法定定密责任人

根据《中华人民共和国保守国家秘密法实施条例》第九条规定："机关、单位负责人为本机关、本单位的定密责任人，根据工作需要，可以指定其他人员为定密责任人。"高校的单位负责人，即校党委书记或校长为学校的法定定密责任人，对学校定密工作负总责，其定密权限基于任职自然享有，与单位定密权限一致。除此之外，法定定密责任人还负责授权指定定密责任人和审批学校的《国家秘密事项范围细目》。

（二）指定定密责任人

指定定密责任人是由法定定密责任人指定、具体承担定密职责的人员。定密工作量较大的高校，可以由法定定密责任人指定人员作为指定定

密责任人，履行定密责任人的职责。

1. 指定定密责任人的范围

鉴于各单位的层级、工作性质和业务范围的差异，《国家秘密定密管理暂行规定》目前没有对指定定密责任人的范围作出统一要求。一般来说，高校的指定定密责任人主要有下列几类人员。

（1）分管涉及国家秘密业务工作的学校副职领导，如学校主管科研或军工科研工作副校长。

（2）产生国家秘密较多的业务主管部门负责人，如党办主任、科技处处长。

（3）经常产生国家秘密事项的业务部门负责人或者工作人员，如有关院系负责人或者项目负责人。

由于对指定定密责任人的级别与数量没有限制，根据工作需要指定定密责任人可以包含以上三类的一类或几类。目前，有些高校授权至党政、科研和教学等学校业务主管部门负责人，有些高校除部处领导外，还授权给院系科研负责人和相关学科方向带头人，还有些高校授权至项目负责人。需要说明的是，各级各类指定定密责任人均需由法定定密责任人直接授权，指定定密责任人无权再行授权。

需要说明的是，未获得定密授权的高校是否需要指定定密责任人，应当根据实际工作需要确定。对于经常知悉、处理国家秘密事项，经常产生派生国家秘密的高校，其法定定密责任人可以指定定密责任人具体开展定密工作；对于很少或从不产生派生国家秘密的高校，可以不专门指定定密责任人，由法定定密责任人具体负责定密工作即可。

2. 指定定密责任人的条件

作为一种特定涉密岗位，定密责任人限定了该岗位任职人员应当符合在涉密岗位工作的基本条件，同时应具备以下履职条件：一是接受定密培训，熟悉保密法律法规及定密规定；二是熟悉本单位主管业务和相关行业工作的保密事项范围；三是熟悉定密程序和方法；四是熟悉本单位业务工作。

3. 指定定密责任人确定程序

指定定密责任人必须严格履行确定程序，一般先由相关涉密业务主管

部门与涉密业务部门提出拟任人选，经学校保密工作机构汇总研究后，提出人选意见，报学校法定定密责任人确定。法定定密责任人在授权指定定密责任人时，应当同时明确其定密权限、定密范围（参见附件4-1），对于学校副职领导，可以指定其在分管业务范围内与法定定密责任人同等的定密权限，对于业务主管部门负责人，可以授权其在业务主管范围同等或较低级别的定密权限，对于业务部门负责人或项目负责人，可以进一步限定其负责业务工作中形成文件以及涉密设备的定密工作。

在实际工作中，学校可能根据工作需要或其他原因，对定密责任人的工作岗位作出调整。定密责任人调整变动的，应当重新履行确定程序。

4. 指定定密责任人的职责

指定定密责任人在职责范围内承担国家秘密确定、变更和解除工作。具体职责如下：

（1）审核批准业务范围内产生的国家秘密的密级、保密期限和知悉范围。

（2）对业务范围内产生的尚在保密期限内的国家秘密进行审核，作出是否变更或者解除的决定。

（3）对是否属于国家秘密和属于何种密级不明确的事项先行拟定密级，并按照规定的程序报上级业务主管部门或保密行政管理部门确定。

此外，在履行上述基本职责的同时，指定定密责任人还根据实际工作需要，承担与定密工作相关的其他工作，包括以下几项：

（1）组织编制《国家秘密事项范围细目》与一览表。

（2）组织进行定密业务指导和培训。

（3）按照申请定密的程序，报请有相应定密权的机关、单位或保密行政管理部门对本单位无权定密的事项进行确定。

（4）对拟公开发布的信息进行保密审查。

（5）受理并答复有关方面提出的定密异议。

（6）就保密事项范围的制定修订或加强和改进定密管理工作，向有关机关提出建议等。

需要说明的是，指定定密责任人在指定范围内具有完全的定密权，在职责范围内作出的确定、变更和解除的国家秘密，具有法律效力，一般情况下，可以不报请法定定密责任人批准，但定密不当的，法定定密责任人有权纠正。

5. 定密责任人的公布和备案

学校应当将定密责任人名单及其定密权限，通过内部文件或者内部公示等书面形式（参见附表 4-2），在学校内部予以公布，以便于相关定密责任人开展定密工作。

同时，学校还应当将定密责任人名单报同级保密行政管理部门（如省国际保密局）备案。定密责任人调整变动的，应当重新履行报备程序。

（三）承办人

承办人，是指根据机关、单位内部岗位职责分工，具体负责处理、办理涉及国家秘密事项的工作人员。在定密工作中，除定密责任人以外，承办人也承担了重要职责。依据保密法律法规，承办人应当对自己承办的事项的国家秘密确定（含密级、保密期限和知悉范围）提出具体意见，并在其形成的载体上做出国家秘密标志，对已确定的国家秘密根据需要作出变更或解密提出意见和建议，提交本单位定密责任人审核批准。定密责任人履行定密职责的方式，就是对承办人提出的确定、变更和解除国家秘密的意见进行审核批准。因此，定密的初始工作由承办人承担，承办人是整个定密流程中第一个环节工作的执行者。

与定密责任人不同的是，承办人是不确定的主体。特别对于涉密程度较高、产生国家秘密事项较多的高校而言，承办人的范围非常广泛，学校不必也无法对承办人进行公示。但是，一旦有关人员作为承办人进入定密程序，就应当具备涉密人员基本资格，产生的涉密事项达到一定数量标准的，应当及时将其纳入涉密人员管理，以确保国家秘密安全。

（四）其他相关人员

高校可以根据本单位保密工作组织设置和工作需要，允许各涉密单位

保密工作主管领导，定密工作小组或有关领域专家等参与定密工作。各涉密单位保密工作主管领导负责组织落实本单位定密工作，对本单位拟定的国家秘密事项进行审核，对国家秘密事项确定、变更、解除工作进行统计，报科技处等定密业务归口管理部门备案；定密工作小组或有关领域专家主要对定密责任人不确定事项提出定密意见，供定密责任人参考。

三、定密培训

鉴于定密是一项政策性、专业性很强的工作，学校应当定期组织开展定密培训，以使定密责任人、承办人与其他相关人员熟悉定密职责和保密事项范围，掌握定密程序和方法，具备做好定密工作的能力。定密责任重、定密事项多的人员应当参加上级业务主管部门或保密行政管理部门组织的定密培训与考核，持证上岗。

为了确保学校法定定密责任人正确履行职责，保密管理办公室应当会同科技处等定密归口管理部门通过发放宣传资料、适时组织教育培训等方式，向法定定密责任人及有关校领导宣传定密知识，使其了解掌握基本的定密专业知识，熟悉与本单位涉密业务工作相关的保密事项范围，为提高学校定密工作的整体水平发挥好领导作用。

四、定密依据、要素与标志

定密依据是各单位确定、变更和解除国家秘密的基本遵循。定密的要素既包括准确描述国家秘密事项名称，也包括准确确定其密级、保密期限与知悉范围。

（一）定密依据

《保密法》划定了国家秘密的基本范围与禁止定密事项，是定密的根本依据。国家秘密及其密级的具体范围（以下简称“保密事项范围”）由国家

保密行政管理部门分别会同中央有关机关,分行业、领域作出具体规定,是定密的直接依据。目前,国家保密局已会同中央有关机关制定实施了90多个保密事项范围,涉及国防、外交、科技、金融等各个行业、领域工作中的国家秘密事项,并对其保密期限、知悉范围作出了明确规定。高校定密工作中经常作为定密依据的文件主要包括《国防科技工业国家秘密范围的规定》(科工安密〔2009〕1488号)与《教育工作中国家秘密及其密级具体范围的规定》(教办〔2017〕3号)。

对承担涉密科研生产任务过程中所产生的国家秘密事项(以下简称“涉密事项”),定密最直接的依据是任务下达单位或者委托方下达的任务书、合同书或项目指南等。针对执行上级机关、单位或者办理其他机关、单位已定密事项所产生的涉密事项的情况,未改变原始秘密基本要素和内容,对已定密事项所承载的信息加以合并、阐释、重述而产生新的信息或载体,依据已定密事项进行定密。

为了使定密工作更具针对性,《武器装备科研生产单位保密资格认定办法》要求各涉密等科研生产单位制定本单位国家秘密范围细目,经法定定密责任人审批后,可以作为本单位相关业务工作的定密依据。

(二)《国家秘密事项范围细目》编制

编制《国家秘密事项范围细目》(以下简称《定密细目》),有利于厘清本单位的涉密事项,便于准确定密和提升定密工作效率,同时也有利于失泄密案件的查处和责任追究。高校在编制《定密细目》时,应当根据本单位的主要涉密科研方向,确定本单位的涉密主体业务范围和相关业务范围,并进一步梳理各涉密业务范围的涉密事项。

1. 编制依据

《定密细目》的编制应当依据《保密法》及其相关法律法规、《国防科技工业国家秘密范围规定》、其他部门或行业关于国家秘密范围的相关规定、军方下达的武器装备科研生产项目时确定的密级、重大专项主管部门确定的密级。

2. 确定主要涉密科研方向的主体业务与相关业务范围

高校应当依据本单位主要涉密科研方向(如核、航天、航空、船舶、兵器、电子等,作为《定密细目》的一级目录),明确本单位开展的涉密主体业务范围与相关业务范围,可能涉及:①军工能力(含动员能力)建设的规划、布局,基础能力建设等;②基础科研、技术基础、民口配套;③民用航天、核能开发、军民共用项目;④为军工主体专业配套的组织、人事、财务、审计等相关业务工作。具体业务范围可以作为《定密细目》的二级目录。

具体涉密业务范围的划定,可参照与学校涉密业务相关的中央有关部委已制定的保密事项范围与细目中的业务范围,适用的采纳,不相关的删减。

3. 编制流程

(1) 以涉密项目为单位,整理国家秘密事项,形成国家秘密事项一览表。

(2) 以课题组为单位,按项目类型梳理国家秘密事项。

(3) 以院系为单位,按业务范围将各类国家秘密事项合理分类。

(4) 以学校为单位,按科研方向,将各业务范围的涉密事项进一步汇总、归类,编制《定密细目》。

(5) 依据保密事项范围,对照国家秘密事项一览表与《定密细目》中国家秘密事项名称、密级、保密期限与知悉范围,梳理、核对、调整、细化学校的《定密细目》中相关信息。

4. 基本方法

(1) 依据国防科技工业保密事项范围及细目,对号入座。

(2) 无号可对,参照同类。

(3) 争议事项,按高限(即密级就高不就低,保密期限就长不就短)确定。

(4) 重大专项,按重大专项密级规定。

(5) 非国防科技工业的涉密事项,按相关保密事项范围对号入座。

5. 注意事项

(1) 确定密级应尽量与定密依据对号入座;

（2）不能对号入座的，也无同类可参照的，应当依据《保密法》，考虑泄密后的危害程度反推；

（3）梳理、细化和确定涉密事项的过程应反复修改、审核；

（4）应注意不同型号的同类涉密事项的差别，或同类涉密事项在不同研制阶段的密级、保密期限的差别；

（5）保密部门应当从宏观层面对各业务领域的定密工作提出指导性建议；

（6）科技管理部门应综合平衡各学科领域所定事项密级水平的高低、细化程度等。

（三）国家秘密事项描述

准确描述国家秘密事项是定密工作的基础。目前保密事项范围与细目中国家秘密事项的描述方式主要有三类："涉密载体"式、"密点"式与"密点＋操作事项"的式。

1. "涉密载体"式

这种描述形式中，中心词为表述"信息载体"名称的名词，如：

（1）＊＊＊配套科研项目的可行性研究报告、合同、执行情况报告、验收文件。

（2）＊＊＊科技实验室评估、验收资料。

（3）＊＊＊的质量保证大纲、分析报告和标准化审查报告。

2. "密点"式

这种描述形式的中心词为表述科研成果形式或信息内容的名词，多数为抽象名词，如：

（1）＊＊＊关键技术、工艺和能力。

（2）特有的＊＊＊处理的新工艺、新技术。

（3）国家重点＊＊＊系统和＊＊＊系统的关键干扰与抗干扰技术、突防技术。

3. "密点＋限定词"式

这种描述形式通过限定词对国家秘密事项进一步限定，如：

(1) ＊＊＊技术/成果应用背景分析。

(2) ＊＊＊技术方案论证＋项目来源(两者同时出现时)。

(3) ＊＊＊技术指标 1＋＊＊＊技术指标 2＋应用背景(三者同时出现时)。

相对来说,第一种描述方式比较笼统、模糊,不符合对项目涉密事项确定具体化、精准化的要求,相对适合于管理部门对保密工作范围界定;第二种描述方式较为清晰,也易操作,被广泛使用;第三种方式最为具体、明确,但需要对相关业务领域保密事项范围深入理解与准确把握。

(四) 定密要素与标志

国家秘密的确定包括密级、保密期限与知悉范围三个要素。国家秘密一经确定,应当在包含国家秘密事项的涉密载体上作出国家秘密标志。

1. 定密要素

国家秘密的密级分为绝密、机密、秘密三级。

国家秘密的保密期限除另有规定外,绝密级不超过 30 年、机密级不超过 20 年、秘密级不超过 10 年,除保密事项范围有明确规定外,保密期限不得确定为长期。国家秘密具体的保密期限一般应当以日、月或者年计,不能确定具体保密期限的,应当确定解密时间或者解密条件。国家秘密的解密条件应当明确、具体、合法。

国家秘密的知悉范围应当根据工作需要限定在最小范围。能够限定到具体人员的,限定到具体人员;不能限定到具体人员的,限定到部门,再由部门限定到具体人员。

2. 国家秘密标志

国家秘密标志形式为“密级★保密期限”“密级★解密时间”或者“密级★解密条件”。涉密载体包含多项国家秘密的,应当依据所包含的涉密事项最高密级、最长保密期限作出标志。国家秘密标志应当与载体不可分离,明显并易于识别。

在纸介质和电子文件国家秘密载体上作出国家秘密标志的,应当符合

有关国家标准或合同甲方约定。没有国家标准且合同甲方无约定的，应当标注在封面左上角或者标题下方的显著位置。光介质、电磁介质等国家秘密载体和属于国家秘密的设备、产品的国家秘密标志，应当标注在壳体及封面、外包装的显著位置。国家秘密的知悉范围应当在国家秘密载体上以主送、抄送的方式或注明文件的传达范围等形式标明。

无法作出或者不宜作出国家秘密标志的，以及不能在载体上直接标明知悉范围的，产生或管理该载体的单位应当以文件批办单等方式书面通知知悉范围内的机关、单位或者人员。凡未标明保密期限或者解密条件，且未作书面通知的国家秘密事项，其保密期限按照绝密级事项 30 年、机密级事项 20 年、秘密级事项 10 年执行。

五、涉密科研项目国家秘密事项的确定、变更与解除

高校涉密科研项目的定密工作主要包括项目所包含国家秘密事项的确定、变更与解除工作，应当坚持“具体化、精准化”原则，做到权责明确、依据充分、程序规范、及时准确，既确保国家秘密安全，又便利信息资源合理利用。

（一）项目国家秘密事项确定

确定项目国家秘密事项通常在项目立项前完成。高校要与任务主管部门或委托方（以下简称“甲方”）充分沟通，尽可能把涉密事项具体化、精准化；如无甲方配合，取得定密授权的高校，可在定密权限内按照学校的定密管理规定和定密程序，依据定密依据，确定涉密事项。同时，应当以涉密事项为源头，按照尽量缩小知悉范围的原则，合理分配研究任务、确定知悉范围，做好本项目的涉密岗位的确定与涉密人员的界定或调整工作，进一步确定并提供涉密人员从事涉密工作所需的符合要求的保密保障条件：涉密计算机、涉密 U 盘等电磁载体、技防物防达标的研究场所等，做好保密体系人、机、载体、场所的动态定密管理。

1. 确定程序

以校科研方面指定定密责任人(以下简称“校科研定密责任人”)设定在学校科研主管部门情况为例,涉密科研项目国家秘密事项确定的一般程序如下:

(1) 在涉密科研项目立项前,课题组项目负责人依据合同书、任务书、保密协议书等约定或相关领域保密事项范围,对涉密项目包含的国家秘密事项(含密级、保密期限与知悉范围)提出拟定意见。

(2) 经院系保密工作主管领导审核后,报校科研定密责任人审批。

(3) 对不确定事项,由校科研定密责任人组织有关领域专家提出定密意见。

(4) 对校科研定密责任人无法确定的事项或超出学校定密授权范围的事项,由高校主管部门报请上级业务主管部门确定。相应流程参见图 4-1 与附表 4-3。

2. 定密注意事项

以下事项不得确定为国家秘密:

(1) 需要社会公众广泛知晓或者参与的。

(2) 属于工作秘密、商业秘密、个人隐私的。

(3) 已经依法公开或者无法控制知悉范围的。

(4) 法律、法规或者国家有关规定要求公开的。

承担涉密科研生产任务过程中所产生的涉密载体,应当由定密承办人依据项目已确定的涉密事项作出标志,并按本单位规定履行相应审批手续。

常用的文件定密审批方式包括以下几项:

(1) 填写文件定密审批单,参见附表 4-4。

(2) 文件定密审批与涉密设备输出审批合二为一,审批事项包含定密信息,审批人含定密责任人。

(3) 在输出的文件上加盖定密章,由定密责任人签字确认。

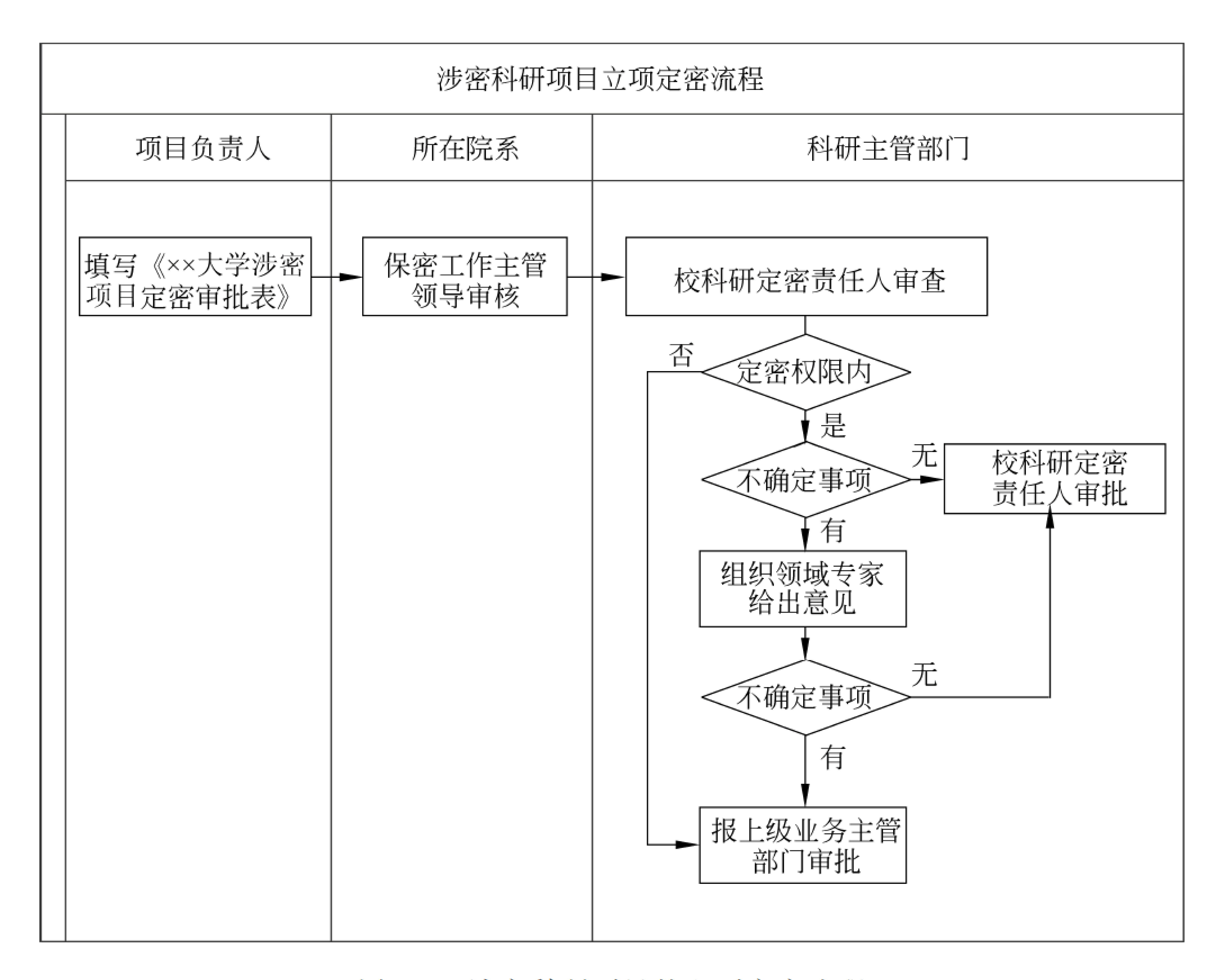


图 4-1 涉密科研项目的立项定密流程

（二）项目国家秘密事项变更

项目国家秘密事项变更包括国家秘密事项的密级、保密期限或知悉范围的变更，一般包括降低密级、延长保密期限及扩大知悉范围。三者既可以单独变更，也可以同时变更。

项目产生的国家秘密事项有下列情形之一的，产生单位（项目依托院系）应当及时提出变更申请，履行变更程序：(1)定密时所依据的法律法规或者保密事项范围发生变化的；(2)泄露后对国家安全和利益的损害程度发生明显变化的。

1. 变更一般程序

（1）由课题组项目负责人提出变更申请；

（2）单位保密工作主管领导填写审核意见后，提交校科研定密责任人审定；

（3）对不确定事项，由校科研定密责任人组织有关领域专家提出意见；

（4）对校科研定密责任人无法确定的事项或超出学校定密授权范围的事项，由高校主管部门报请上级业务主管部门或者保密行政管理部门确定。

相应流程与表格参见图 4-2 与附表 4-5。

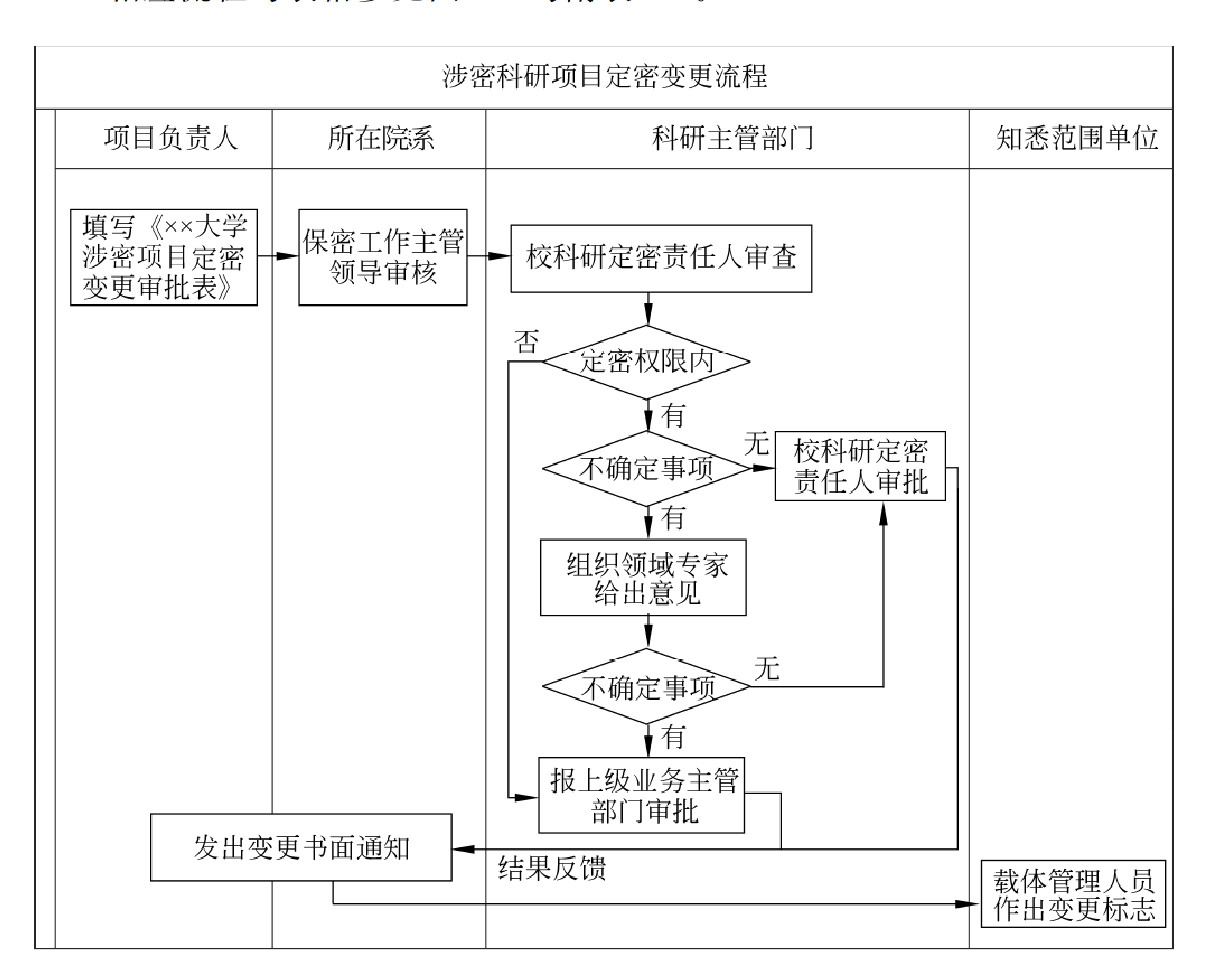


图 4-2　涉密科研项目的定密变更审批流程

变更需要延长保密期限的，应当在保密期限届满前六个月提出变更申请；延长保密期限使累计保密期限超过保密事项范围规定的，还应当报规定该保密事项范围的中央有关机关批准。

2. 变更通知与标识

变更审批通过后，提出单位将变更情况书面通知知悉范围内的机关、单位。延长保密期限的书面通知，应当于原定保密期限届满前送达知悉范围内的机关、单位或者人员；国家秘密事项（载体）管理人员收到变更通知后，应当在载体原国家秘密标志附近作出变更标志，并标明变更后情况与变更时间。

3. 变更注意事项

除原定密机关、单位或者上级机关外，其他机关、单位无权变更不属于其职权范围的国家秘密的密级、保密期限和知悉范围。

扩大涉密载体知悉范围一般不需走变更审批流程。不在知悉范围内的学校内部人员因工作需要确需知悉的，应当经项目负责人批准；项目负责人退休或离职的，应当经单位保密工作主管领导批准；学校外部人员因工作需要确需知悉的，应当经原定密机关、单位同意。国家秘密事项（载体）管理人员对知悉范围外人员的使用情况应当作出详细记录。原定密机关、单位对扩大知悉范围有明确规定的，应当遵守其规定。

（三）项目涉密事项解除

项目涉密事项的解除主要包括自行解密与提前解密两种情况。

1. 自行解密

高校各单位自主产生的国家秘密事项（通常以载体形式呈现）的具体保密期限已满、解密时间已到或者符合解密条件的，自行解密。自行解密一般由高校科研定密主管部门每年定期组织，由高校所属各单位梳理并审查后报相关定密责任人审批，可以一事一办（参见附表 4-6），也可以汇总办理（参见附表 4-7）。

2. 提前解密

对各单位产生的尚在保密期限内的国家秘密事项（载体），有下列情形之一的，应当根据情况变化及时提前解除密级：(1)保密法律法规或者保密事项范围调整后，不再属于国家秘密的；(2)公开后不会损害国家安全和利

益，不需要继续保密的。保密事项范围明确规定保密期限为长期的国家秘密事项提前解密，还应当报请规定该保密事项范围的中央有关机关批准。提前解除程序参见图 4-3。

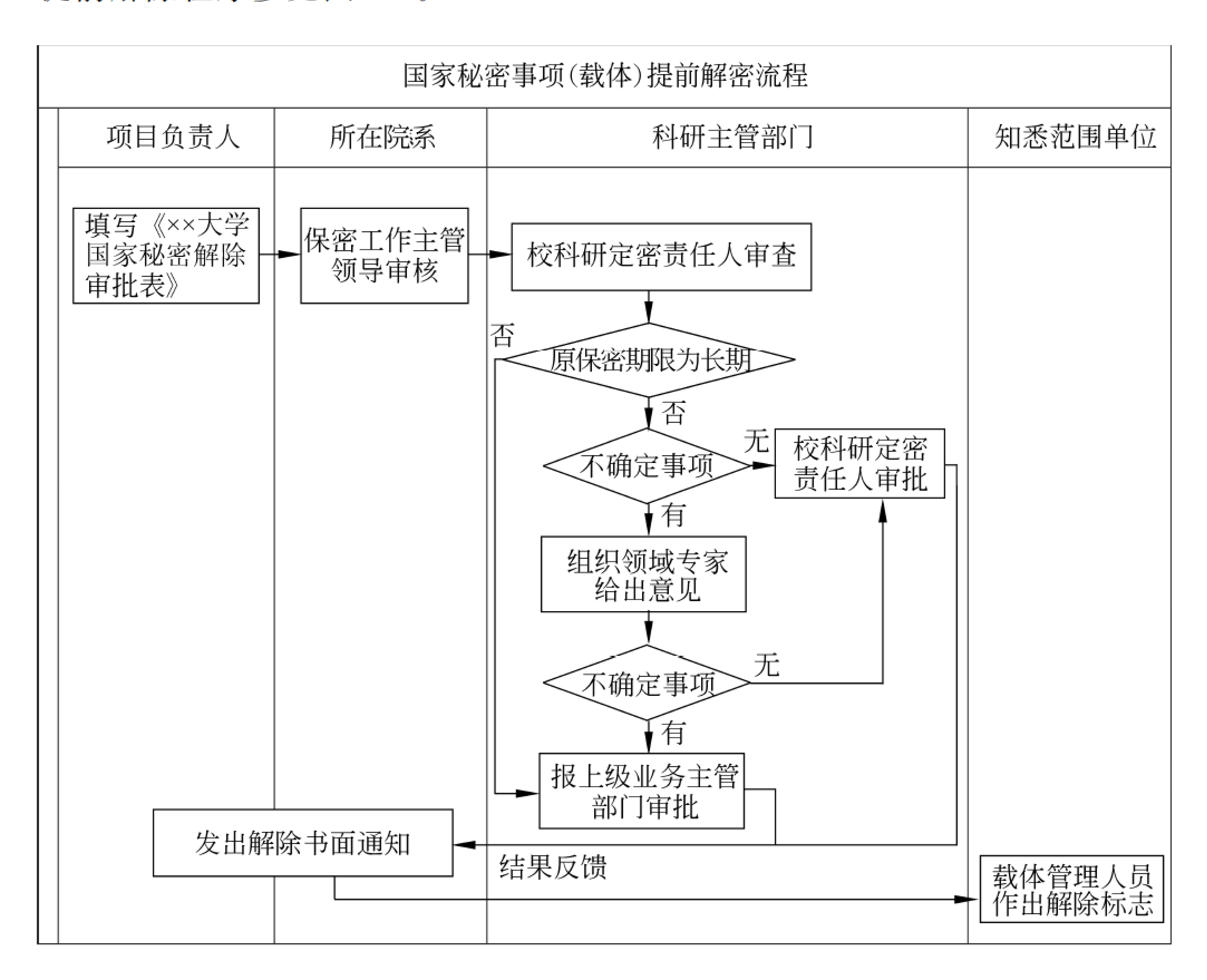


图 4-3　国家秘密事项提前解密流程

3. 解除通知与标识

对批准解除的国家秘密事项(载体)，由产生单位书面通知知悉范围内的机关、单位或人员，产生单位或原定密机关、单位或其上级机关正式公布的，视同书面通知；各单位国家秘密事项(载体)管理人员收到解密通知后，应当在载体原国家秘密标志附近作出解密标志，并注明解密时间。

4. 解密与公开

解密不等于公开。国家秘密事项解除后按照内部事项进行管理。公

开由学校自主产生的已解密国家秘密事项，应当履行解密文件公开保密审查相关手续，参见附表 4-8。

公开其他已解密国家秘密事项，应当经原定密机关、单位或其上级机关、相关单位同意。公开时不得保留国家秘密标志，对国家秘密标志以及属于敏感信息的内容，应当作删除、遮盖等处理。

5. 解密注意事项

（1）对于已到保密期限，但原定密单位或其上级机关、单位要求继续保密的事项，应根据延长保密期限通知作出保密期限变更标识，在所要求的时间内不得解密。

（2）对在保密范围中已经规定最短保密期限的，解密时间不得短于规定时间，确需短于规定时间解密的，应报上级机关或有关业务主管部门批准。

（3）保密事项范围明确规定保密期限为长期的，学校不能擅自解密；确需解密的，应当上报规定该保密事项范围的中央有关机关批准。

（4）原确定密级的机关、单位撤销，有关解密和变更事项由承担原职能的机关、单位负责；无相应机关、单位的，由有关上级机关或保密行政管理部门指定的单位负责。

附件 4-1　定密责任人授权书示例

定密责任人授权书

根据《中华人民共和国保守国家秘密法》及有关规定，为规范学校科研定密工作，特授权____________为定密责任人，依法履行职权范围内的定密职责。

定密权限：绝密级（　）、机密级（　）、秘密级（　）；

定密范围：

全校/某院系涉密科研项目国家秘密事项（　）；

全校/某院系部处国家秘密载体（　）；

全校/某院系部处涉密设备（　）。

本授权书的权责将随着被授权人岗位调整而自行变更、终止。

本授权书一式三份，授权人、被授权人各持一份，一份交本单位保密管理办公室备案。

授权人：（签字）　　　　　　　　　　机关、单位名称：（盖章）

年　　月　　日

附表 4-2　定密责任人确定情况汇总表示例

定密责任人确定情况汇总表

机关、单位(盖章)：　　　　　　　　　　　　　　填表日期：　　　年　　月　　日

序号	姓 名	岗 位	定密权限	定密范围	类别
1					
2					
3					
4					
5					

注：“类别”填写法定或者指定。

附表 4-3　＊＊大学涉密项目定密审批表示例

＊＊大学涉密项目定密审批表

<table>
<tr><td>项目名称</td><td colspan="3"></td><td>密级及期限</td><td></td></tr>
<tr><td>院　　系</td><td colspan="3"></td><td>负责人</td><td></td></tr>
<tr><td>定密依据</td><td colspan="5">1. 合同书、任务书、保密协议书等约定　（　）
2.《＊＊大学国家秘密事项范围细目》第　类第　号　（　）
3.《国防科技工业国家秘密范围目录》第　类第　号　（　）
4. 其他有关行业《国家秘密及其密级具体范围的规定》：　（　）</td></tr>
<tr><td colspan="6">项目包含国家秘密事项</td></tr>
<tr><td>序号</td><td colspan="2">国家秘密事项名称</td><td>密级</td><td>保密期限</td><td>知悉范围(需具体到人)</td></tr>
<tr><td>1</td><td colspan="2"></td><td></td><td></td><td></td></tr>
<tr><td>2</td><td colspan="2"></td><td></td><td></td><td></td></tr>
<tr><td colspan="6">项目负责人签字：　　年　月　日</td></tr>
<tr><td colspan="2">院系保密工作主管领导审查意见</td><td colspan="4">负责人签字：　　年　月　日</td></tr>
<tr><td colspan="2">校科研
定密责任人意见</td><td colspan="4">□同意以上密级确定意见。
□组织有关领域专家提出定密意见。
□报请上级业务主管部门确定。
签字：　　年　月　日</td></tr>
</table>

附表 4-4 ＊＊大学文件定密审批单示例

＊＊大学文件定密审批单

文　件　标　题			
包含涉密事项			
拟定密级		保密期限	
知悉范围			
定密依据	1. 所执行或者办理的已标密文件　（　） 2. 背景项目定密审批表　（　） 3.《＊＊大学国家秘密事项范围细目》　（　） 承办人签字： 年　月　日		
定密责任人意见	签字：　年　月　日		

附表 4-5　＊＊大学涉密项目定密变更审批表示例

＊＊大学涉密项目定密变更审批表

<table>
<tr><td colspan="2">项目名称</td><td colspan="3"></td><td colspan="2">当前密级及期限</td><td></td></tr>
<tr><td colspan="2">院　　系</td><td colspan="3"></td><td colspan="2">负责人</td><td></td></tr>
<tr><td colspan="5">原“＊＊大学涉密项目定密审批表”编号</td><td colspan="3"></td></tr>
<tr><td colspan="2">定密变更事项</td><td colspan="6">1. 新增国家秘密事项（　）
2. 原定国家秘密事项密级变更（　）
3. 保密期限变更（　）
4. 知悉范围变更（　）</td></tr>
<tr><td colspan="2">定密变更依据</td><td colspan="6">1. 项目密级或期限变更（　　）
2. 有关行业或学校“国家秘密事项范围”调整（　　）
3. 工作岗位调整（　　）
4. 其他：（　　）</td></tr>
<tr><td colspan="8">变更后项目包含国家秘密事项情况</td></tr>
<tr><td>序号</td><td colspan="3">国家秘密事项名称</td><td>密级</td><td>保密期限</td><td colspan="2">知悉范围（需具体到人）</td></tr>
<tr><td>1</td><td colspan="3"></td><td></td><td></td><td colspan="2"></td></tr>
<tr><td>2</td><td colspan="3"></td><td></td><td></td><td colspan="2"></td></tr>
<tr><td colspan="8">项目负责人签字：　　　　年　　月　　日</td></tr>
<tr><td colspan="3">院系保密工作主管领导审查意见</td><td colspan="5">负责人签字：　　　年　　月　　日</td></tr>
<tr><td colspan="3">校科研定密责任人意见</td><td colspan="5">□ 同意以上密级变更意见。
□ 组织有关领域专家提出变更意见。
□ 报请上级业务主管部门确定。
签字：　　　年　　月　　日</td></tr>
</table>

附表 4-6　＊＊大学载体自行解密审批表示例

＊＊大学载体自行解密审批表

编号：

载体名称		载体产生时间	
载体密级	□秘密　□机密　□绝密	保密期限 /解密时间 /解密条件	
是否满足自行解密条件	□是　□否		
承办人意见	解密后拟处理方式　□长期内部　□公开 签字： 年　月　日		
定密责任人审定意见	签字：　年　月　日		

注：解密后申请公开的载体另行办理审批手续。

附表 4-7　＊＊大学涉密载体自行解密审批表示例

＊＊大学涉密载体自行解密审批表

________年度

单位：

载体名称	载体编号	载体来源	密级及期限	产生日期	到期日期	申请解密时间	解密后拟处理方式 1. 长期内部 2. 公开	承办人
定密责任人意见	□同意解密及解密后处理方式　　□其他 签字：　年　月　日							

注：解密后申请公开的载体另行办理审批手续。

附表 4-8　＊＊大学解密文件公开前保密审查表示例

＊＊大学解密文件公开前保密审查表

编号：

文件产生部门(单位)		文件产生时间	
文件名称			
文件密级	□秘密　□机密 □绝密	保密期限 /解密时间 /解密条件	
是否满足法定解密条件	□是　□否		
解密后 拟公开原因			
需去除的敏感内容	1. 国家秘密/解密/变更标识 2. 其他内容：		
承办人意见	□以上情况属实 □其他： 单位业务主管或项目 负责人签字：　　年　月　日		
院(系)部处保密主管领导意见	□ 同意去除敏感内容后公开 □ 其他： 负责人签字：　　年　月　日		

第五章　科研人员保密管理

科研保密管理涵盖学校方方面面的工作，归根到底是对人的管理。科研人员是科研工作中最为重要的要素，是国家科技秘密的直接生产者，是科研保密管理的第一要素。因此，涉密科研人员管理一直是保密监督管理的核心内容。

本章主要从保密宣传教育、涉密科研人员全过程保密管理以及参与涉密科研工作的各类科研人员的保密管理重点三方面加以阐述。

一、保密宣传教育

作为国家安全教育的重要内容，保密宣传教育是高校保密工作一项基础性、长期性的工作。随着国际化办学和尖端科研的迅猛发展，高校国家安全工作面临严峻挑战。在这种形势下，更要准确把握国家安全形势的新特点、新趋势，强化国家安全意识，提高防范意识与能力，做好开放环境下的保密工作，维护国家利益。为了使保密教育培训具有针对性和实效性，高校应当遵循“按需施教、务求实效”的原则，根据学校发展需要和不同岗位人员的多样化培训需求，分层次、分类别地开展保密宣传教育。

（一）培训要求

保密培训要求主要来源于以下三个方面：

（1）所在地区保密行政管理部门与教育部等上级主管部门的保密培训

要求，比如保密宣传教育周、国家安全教育日等相关培训要求。

（2）《武器装备科研生产单位保密资格审查认定管理办法》以及《关于进一步加强涉密人员保密管理工作的意见》（国保发〔2015〕5号）等文件对涉密人员提出明确的培训要求，主要包括：

① 非涉密人员进入涉密岗位前应接受学校或所在单位组织的专门的保密培训并通过考试；

② 涉密人员在岗期间参加有组织的保密教育培训，一级、二级保密资格单位，每人每年度不少于15学时，三级保密资格单位，每人每年度不少于8学时；

③ 涉密人员脱离涉密岗位前应接受专门的保密提醒；

④ 涉密人员因公因私出国（境）前应接受专门的保密提醒；

⑤ 学校及院系所专兼职保密管理人员应参加上级部门组织的上岗培训，取得上岗资格。

（3）学校结合队伍建设与人才培养的需要，对各类人员提出明确的培训需求，一般包括：

① 将保密教育列入学校党委理论学习中心组学习内容；

② 将保密教育列入新入职干部、新入职人员岗前培训内容；

③ 将保密教育列入新入校研究生与本科生入学教育内容；

④ 将保密教育列入中层干部年度培训内容；

⑤ 国防生每年接受例行保密教育。

此外，为了持续提高各类人员的保密意识，诸多高校把保密教育融入各种大型会议与重要活动中，利用各种机会对与会人员进行保密提醒。

（二）职责与分工

学校各单位、各部门根据各自主管业务的不同，在保密宣传教育中各司其职、分工合作。一般来说，学校保密管理办公室负责统筹协调组织校级保密宣传教育活动，监督、指导学校各单位的保密宣传教育工作，并为各单位提供培训资料、教材、教学及咨询等保障；各单位负责组织开展本单位

及主管业务的保密宣传教育活动，如人事处负责组织开展涉密人员和新入职人员的保密宣传教育，组织部负责组织开展中层干部例行保密宣传教育以及新任中层干部岗前保密培训，研究生工作部、学生处分别负责组织开展研究生、本科生新生入学保密教育，各院系组织开展本院系的保密教育培训，各项目负责人负责落实本课题组的保密培训教育工作。

（三）教育培训计划

为了增加保密教育培训的计划性，每年年初或春季学期初，学校保密管理办公室结合国家保密形势、上级保密工作要求、学校年度保密工作重点以及各部门培训需求，制订学校年度保密培训计划，对培训时间、培训对象、培训教师、培训内容与培训方式等作出安排，参见表 5-1。学校所属各单位从人才培养、科技创新、项目需求及内部建设等角度出发制订部门年度保密培训计划，并报保密管理办公室备案。

表 5-1　保密培训计划表及填写示例

序号	组织单位	业务培训名称	培训目的	培训内容	学期	学时	方式	任课教师	培训对象
1	人事处保密办	保密形势和案例警示教育	提高法制观念和保密意识，筑牢保密防线	保密形势、反间防间、泄密案例教育	春季	3	讲课	邀请专家	全体涉密人员
2	人事处保密办科技处	涉密项目保密管理知识	熟悉涉密项目保密管理办法，明确管理流程	宣贯涉密项目保密管理办法	春季	2	讲课	科技处保密主管	涉密项目负责人与管理人员
3	研究生院保密办	研究生专项培训	加强涉密课题组研究生保密意识和防范能力	相关规定、失泄密案例、防范技术	秋季	2	讲课	保密办主管	涉密课题组研究生
4	信息办保密办	信息安全培训	强化信息安全意识，提高防范能力	失泄密案例、保密管理要求与技术防范措施	秋季	3	演示	信息安全专家	全体涉密人员

保密教育培训内容一般包括以下几项：

（1）保密工作方针政策教育。

（2）保密法律、法规，学校保密管理规章制度宣传教育。

（3）保密工作形势教育。

（4）保密工作先进事迹和泄密典型案例警示教育。

（5）保密知识技能与保密技术防范措施教育。

（6）上级部门要求的其他保密宣传教育内容。

为了使培训更具针对性，应当根据培训对象和培训目标的不同，安排相应的培训内容，比如，针对中层干部的培训，以提高保密依法行政、依法管理能力为目标，侧重进行保密工作方针政策和保密法律法规、规章制度等方面的宣传教育；针对专兼职保密管理人员的培训，以提高保密管理工作能力为目标，侧重组织上岗培训和保密知识技能与保密技术防范措施教育等方面的培训；针对涉密项目负责人的培训，以提高保密意识、掌握保密管理要求为目标，侧重组织泄密典型案例警示教育、保密知识技能与保密技术防范措施等方面的教育培训。

为了提高保密教育培训的有效性，培训内容的设计可以考虑与各类人员的业务工作流程相结合，比如，鉴于中层干部经常代表学校参加各类对外交流活动，可以结合对外交流对象、交流事项等，识别保密管理主要风险，提出针对性保密管理措施与建议等；涉密项目负责人可以结合相关科研活动，包括从项目申报到结题的执行过程，对外交流、发表文章、指导学生等活动，分析各个环节存在的主要失泄密风险，提出对应的保密管理措施。

保密宣传教育形式灵活多样，不拘一格。主要形式一般包括：

（1）举办专题性或者综合性保密知识讲座、研讨班。

（2）组织保密知识测试或竞赛活动。

（3）通过工作会、研讨会、座谈会、报告会等各类会议形式通报保密工作形势、部署保密工作任务，或者结合业务工作会议提出保密要求，进行保密宣传教育。

（4）举办保密宣传教育展览，设置保密知识宣传栏，进行保密防范措施多媒体技术演示。

(5) 发放保密宣传教育学习资料，利用网络以及微信公众号等新媒体推送保密宣传教育信息等。

培训以在学校内部开展为主，也可根据需要选派人员参加校外专业机构组织的培训，或外请专家到校进行培训。

(四) 教育培训实施

根据学校或部门年度保密培训计划，保密管理办公室及各单位组织开展培训，并根据实际工作和培训需求的变化，对培训计划实施动态管理，及时调整，并保留保密教育培训计划、通知、签到表、培训教材资料、考试卷等保密教育记录。

为了提高保密宣传教育的有效性，可以适时开展培训有效性评价(参见附表 5-1)，根据反馈意见及时调整培训安排。同时，关注以下几方面：

1. 保密宣传教育与业务工作相结合

学校相关管理部门可以将保密培训教育分别列为本科生、研究生入学教育，新教工入职教育、博士后进站培训以及新干部岗前培训等的重要必备内容之一；涉密课题组把保密提醒作为每次例会的必备内容；院系把保密培训列入院系教职工大会内容；组织部把保密提醒与教育列入每次党政干部会议内容，等等。这样不但提高保密宣传教育的受众面，还有助于将保密要求融入业务工作中，降低组织开展保密培训的时间、人力等成本。

2. 广泛宣传和重点教育相结合

学校可以通过举办保密宣传图片展、利用闭路电视播放保密宣传教育片、通过校园网宣传保密基础知识等多种形式开展全员保密教育；针对涉密人员，学校、院系、课题组分层次开展有针对性、持续性的保密培训和教育：(1)学校层面，主要关注共性需求；(2)院系层面，充分结合本单位保密工作的特点与薄弱环节，组织有针对性的培训，推动保密规章制度在本单位的落地；(3)课题组层面，结合涉密项目的保密要点及保密检查时发现的问题，开展更具体的培训，确保课题组保密工作符合学校、院系保密管理的要求。

3. 普适性与特殊性相结合

结合国家保密形势、年度保密工作要求与学校保密工作特点，制订普

适性与特殊性兼顾的保密培训计划：(1)面向全校师生或各单位全体教职员工的培训，以保密形势、国家法律法规、保密基本防范常识为主，旨在增强全员保密意识，掌握保密常识；(2)面向领导层的培训，以保密形势、国家法律法规、上级部门保密管理要求为主，提高对保密工作重要性的认识，增强落实保密责任的自觉性；(3)面向保密管理人员的培训，以学校保密工作规章制度、保密管理流程与操作规范为主，提高管理者的业务水平和操作技能，增强严格履行岗位职责的能力；(4)面向涉密专业技术人员的培训，以失泄密典型案例、保密工作基础知识与应知应会为主，提高保密意识，增强防范能力；(5)面向学生特别是可能接触国家秘密的学生的保密教育培训，重点做好学生出国(境)前保密提醒和防策反教育，提高学生的保密意识与能力。

二、涉密科研人员保密管理

涉密科研人员是指由于科研工作需要，在涉密科研岗位合法接触、知悉或经管国家秘密事项的人员。学校对涉密科研人员的上岗、在岗、离岗等全过程实行严格管理。上岗前管理主要包括涉密岗位和涉密等级的确定、涉密人员资格审查与密级界定、岗前培训等环节；在岗管理主要包括保密教育培训、保密监督检查、出国(境)与涉外活动管理以及保密补贴与考核奖惩等环节；离岗管理主要包括脱密期管理。

（一）职责与分工

按照“业务工作谁主管、保密工作谁负责”的原则，学校人事处是全校涉密人员的归口管理部门；涉密岗位所属单位负责日常管理；保密管理办公室对涉密人员管理进行指导监督检查，并根据日常管理情况及保密检查情况向保密委员会提出奖惩建议。管理内容主要包括以下内容：

(1) 涉密人员上岗、在岗、离岗管理以及涉密人员信息的管理。

(2) 向公安机关出入境管理部门登记备案涉密人员变动情况。

(3) 涉密人员因私出国(境)相关管理工作及证件管理。

(4) 组织实施涉密人员保密教育培训,组织新入职人员的保密宣传教育。

(5) 发放涉密人员保密补贴。

(6) 组织涉密人员年度考核等。

(二) 涉密岗位界定

涉密岗位是指因工作需要,在科研、管理等日常工作中,产生、经管或者经常接触、知悉国家秘密事项的岗位。

1. 涉密岗位类别

根据岗位属性,涉密岗位一般可以分为特定涉密岗位和量化涉密岗位。根据有关文件规定,特定涉密岗位包括以下几种:

(1) 制作、复制、收发、传递、保管、维修和销毁国家秘密载体的岗位。

(2) 涉密信息系统有关建设、管理、运维等岗位。

(3) 承担涉密项目研究、建设、管理任务的岗位。

(4) 从事密品生产的岗位以及相关管理岗位。

(5) 定密责任人岗位。

(6) 其他专门处理国家秘密的岗位,如军口专家、专家组工作人员。

除以上特定岗位,在工作中产生、处理国家秘密达到一定数量的岗位,也应当确定为涉密岗位。包括工作中产生、处理绝密级或机密级国家秘密事项的岗位以及近三年年均产生、处理秘密级国家秘密事项 9 项(件)以上的岗位。

2. 涉密岗位密级确定

根据涉及的国家秘密事项范围与涉密程度不同,涉密岗位分为核心涉密岗位、重要涉密岗位和一般涉密岗位三个等级。核心涉密岗位是指日常工作中产生、经管或者经常接触、知悉绝密级国家秘密事项的关键工作岗位,主要包括以下几种:

(1) 从事绝密级国家武器装备重点型号研制、生产、技术、管理的工程

总指挥、总设计师、总工程师、总质量师等重要岗位。

（2）国家绝密级科研项目负责人岗位、核心技术人员岗位。

（3）经管绝密级文件、资料、档案的管理岗位。

（4）在近三年工作中年均产生、处理绝密级国家秘密事项 3 项（件）以上的岗位。

（5）其他经国家秘密事项密级确定机关、单位限定和学校依据相关法规批准的掌握和知悉绝密级国家秘密的岗位。

重要涉密岗位是日常工作中产生、经管或者经常接触、知悉机密级国家秘密事项的重要工作岗位，主要包括几下几种：

（1）从事机密级国家武器装备重点型号研制生产的项目负责人，关键技术、管理岗位。

（2）机密级科研项目负责人岗位、核心技术岗位。

（3）经常接触、知悉机密级事项的学校、院系、部处主要领导岗位。

（4）学校涉密计算机安全保密管理员。

（5）经管机密级文件、资料、档案的管理岗位。

（6）近三年工作中年均产生、处理绝密级国家秘密事项不足 3 项（件）或者机密级国家秘密事项 6 项（件）以上的岗位。

（7）其他经国家秘密事项密级确定机关、单位限定和学校依据相关法规批准的掌握、知悉机密级及少量绝密级国家秘密的岗位。

一般涉密岗位是日常工作中产生、经管或者经常接触、知悉秘密级国家秘密事项的工作岗位，主要包括以下几种：

（1）从事秘密级科研项目负责人岗位、核心技术人员岗位。

（2）经常接触、知悉秘密级事项的业务主管部门主要领导岗位。

（3）从事秘密级科研任务的各单位涉密计算机安全保密管理员。

（4）经管秘密级文件、资料、档案的管理岗位。

（5）近三年工作中年均产生、处理机密级国家秘密事项不足 6 项（件）或者秘密级国家秘密事项 9 项（件）以上的岗位。

（6）其他经国家秘密事项密级确定机关、单位限定和学校依据相关法

规批准的掌握、知悉秘密级及少量机密级国家秘密的岗位。

不属于特定涉密岗位，年均产生、处理秘密级国家秘密事项不足9项（件）的岗位可以不界定为涉密岗位。对不在涉密岗位工作，但又接触或者知悉少量国家秘密的人员，可以不确定为涉密人员，可通过开展保密培训教育、签订保密承诺书等方式对其进行保密管理。

（三）涉密人员上岗前保密审查

对拟进入涉密岗位、从事涉密工作的人员，必须按照“先审查、后使用”的原则事先进行资格审查。涉密岗位工作的人员应当具备以下基本条件：

（1）具有中华人民共和国国籍，无境外永久居留权或长期居留许可，与境外人员（含港澳台）无婚姻关系。

（2）热爱祖国，拥护中国共产党的领导。

（3）遵纪守法，无违法犯罪和违纪违规记录。

（4）作风正派，品行端正，无不良嗜好。

（5）忠诚可靠，历史和境外亲友关系清楚；

（6）忠于职守，有较强的责任心和事业心。

（7）具有涉密岗位要求的工作素质和工作能力。

（8）无其他可能影响国家安全利益的倾向。

有下列情形之一的人员不得任（聘）用为涉密人员：

（1）有强制戒毒、收容、拘留、劳动教养或刑事处罚记录的。

（2）有故意泄露国家秘密的记录或因过失泄露国家秘密受到党内警告或行政记过及以上处分的。

（3）年度考核不合格的。

（4）直系亲属或配偶在境外组织、机构工作的。

（5）有移居境外或长期出境意向的。

（6）临时招聘或暂时借用的。

（7）其他经保密管理办公室认定不适宜的。

配偶与子女均已移居国(境)外,不得任(聘)用到核心、重要涉密岗位。考虑到学生的流动性,原则上禁止本科生参与涉及国家秘密的科研、生产工作,禁止任(聘)用研究生到核心、重要涉密岗位,工作去向确定、单位可靠的人员除外。

所有承担涉密任务、进入涉密岗位的人员均须经过严格的审查,并对审核情况做出文字记载。未经涉密资格审查的任何人员,不得从事涉密工作。

涉密人员上岗前保密审查流程参见图 5-1。审查内容主要包括:国籍、政治立场、个人品行、学习经历、工作经历、现实表现、主要社会关系以及与国(境)外组织和人员交往情况。拟上岗人员除填写资格审查表(参见附表 5-2),还应当提供户籍证明、身份证、婚姻证明及配偶信息等相关证明材料。为了保证国家秘密安全,对拟进入重要或核心涉密岗位人员,以及有国外留学或工作背景或经历复杂者,由学校保卫处等对口部处提请公安机关和国家安全机关对其进行国家安全背景审查。审查不合格的,不得任(聘)用到涉密岗位工作。

资格审查通过者,由保密管理办公室或涉密岗位所属单位对其进行岗前培训及考试。上岗前保密培训的目的是使拟进入涉密岗位人员初步建立保密意识,掌握基本的保密知识技能。培训的主要内容是国家及学校保密形势、拟进入的涉密岗位主要涉及的保密事项、学校和二级单位保密规章制度以及保密基本知识技能等。培训后应当组织考核,未经培训或者考核不合格者,不得任(聘)用到涉密岗位工作。

为了保证上岗前保密培训的效果,可以采取分层培训的方式,即由所在单位保密工作领导小组通过发放学习材料以及谈话等方式及时组织岗前保密培训及考试,由学校保密管理办公室定期(每周或每个月)对新上岗人员进行系统培训。

(四)涉密人员密级界定

对涉密科研人员,应当按照“以项目定岗、以岗位定人”“尽量缩小知密

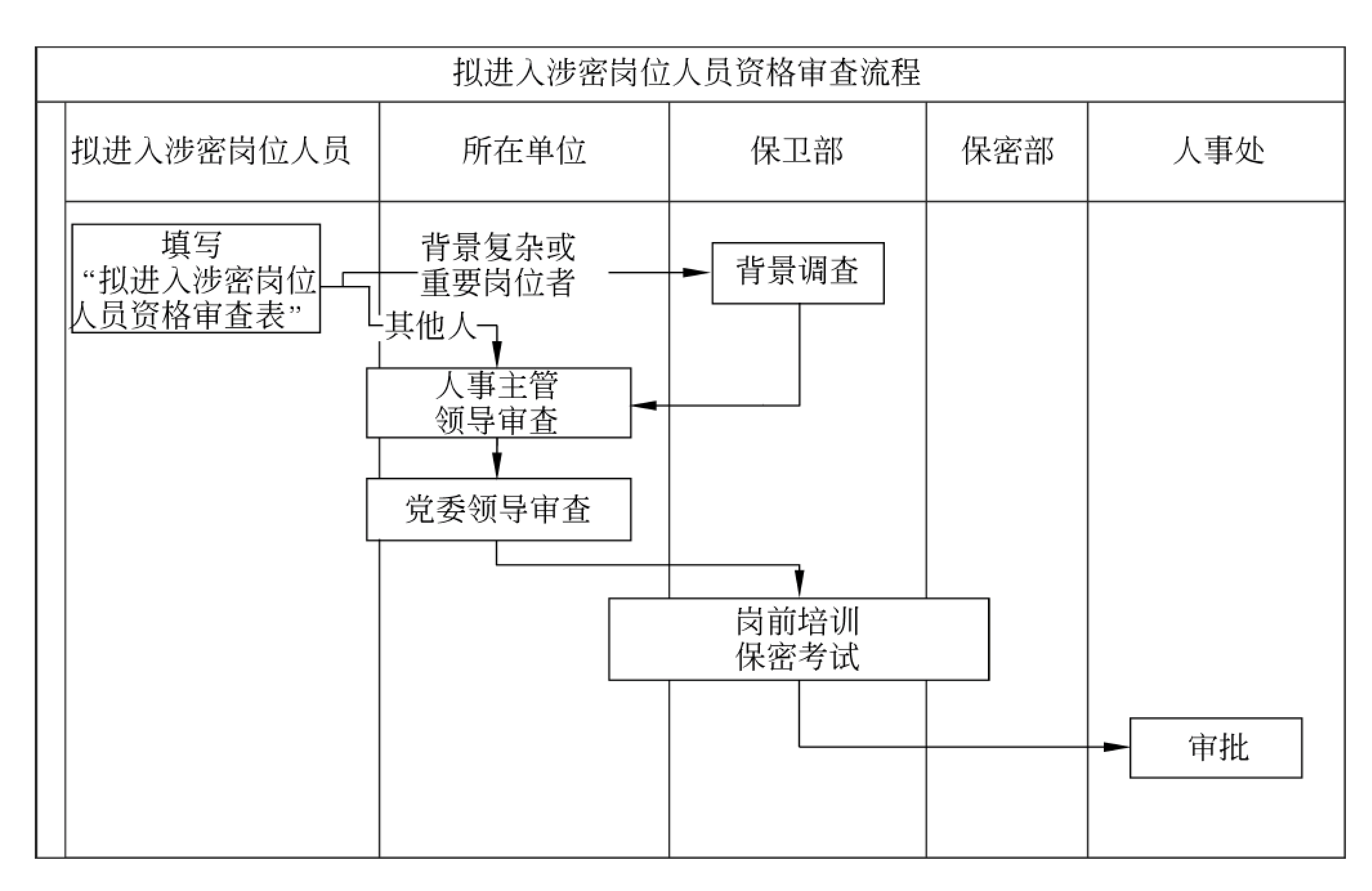


图 5-1　拟进入涉密岗位人员资格审查流程

范围”的原则，由项目负责人在签订涉密项目合同前，依据项目的涉密事项和知悉范围确定涉密岗位及拟承担人员，由学校人事处通过综合分析该人员承担的涉密岗位情况，界定其涉密等级。对涉密管理人员，则根据其承担涉密岗位的密级确定其涉密等级。

1．界定原则

（1）在核心涉密岗位工作的人员应确定为核心涉密人员；在重要涉密岗位工作的人员应确定为重要涉密人员；在一般涉密岗位工作的人员应当确定为一般涉密人员。

（2）对同时在两个（或以上）涉密岗位工作的涉密人员，依照所承担岗位中涉密等级最高的岗位界定。

（3）只接触绝密级、机密级国家秘密载体但不知悉内容的涉密人员，涉密等级可以下调一级（如机要收发人员）。

（4）确因工作需要进入涉密岗位的研究生，原则上只能承担一般涉密岗位工作。对机密级项目，由课题组或项目负责人采取分段安排任务、回

避核心技术等方法进行技术降密处理。

2．密级界定与调整

由涉密人员填写密级审定表(参见附表5-3),经其所在二级单位根据审定原则审核、报人事处审批。审批通过后,为了使重要或核心涉密人员深刻了解保密工作特点,充分认识所承担的保密责任,在其上岗前一般由人事处或保密管理办公室负责人对其进行保密谈话。

按要求,涉密人员上岗前还应当签订保密承诺书,上交学校人事处因私护照、港澳通行证、台湾通行证等因私出国(境)证件。

对通过审查和培训,界定涉密等级并签订保密承诺书、上交因私证件的涉密人员,人事处应当发放上岗通知书或上岗证,并为其建立“一人一档”的管理档案,将其纳入学校涉密人员总台账。

当涉密岗位发生变化或者涉密岗位涉密等级调整时,涉密人员的涉密等级根据界定原则应当及时调整,并同时移交本岗位不再使用或不宜保管的涉密设备、存储介质或涉密载体。比如,涉密人员的涉密岗位由技术岗位调整为管理岗位时,或由重要涉密岗位调整为一般涉密岗位时,其原来合法持有的涉密技术文件或者机密级文件应当及时办理移交手续。

对脱密后拟再次进入涉密岗位的人员,如已过脱密期,应对照初次进入涉密岗位人员密级的审定程序办理上岗手续;如尚在脱密期内,可适当简化资格审查及岗前培训环节。

对到校挂职、借调、交流、实习等人员需要进入涉密岗位的,参照上述要求执行。资格审查可委托其人事关系所在单位进行。

学校人事处或组织部等部门定期将涉密人员名单(含处于脱密期人员名单)及变化情况(新增涉密人员名单及脱密期满人员名单)报所在地区公安机关出入境管理机构备案。在挂职借调、交流、实习期间确认为涉密人员的外单位人员,应当通知原单位进行备案,原单位不具备备案条件的,由学校进行备案。学校还可以通过公安机关出入境管理机构提供的本单位涉密人员出入境记录,核查其出国(境)证件上交情况。

涉密人员在岗期间及脱密期满之前,均不得在本人涉密领域内从事第

二职业，不得在境外或其驻华机构任职，也不得为这些机构、组织提供各种咨询服务。

（五）涉密人员在岗保密管理

涉密人员在岗期间，一方面要持续对其进行保密教育培训，不断强化其保密意识、增强其管理国家秘密的保密能力，一方面通过定期、不定期的保密检查与奖惩，督促、引导其自觉遵守保密规章制度，特别要对其涉外活动进行重点监管。

涉密人员所在单位对其承担日常监管的职责，通过考察其政治态度、思想状况和工作表现，对认真履行保密义务，遵守保密制度的涉密人员，按时发放保密补贴；对不适合继续在涉密岗位工作的人员，报告学校保密管理办公室与人事处，及时调离涉密岗位。

1. 涉外活动监管

涉外活动包括在境内外参加有境外机构、组织、人员参与的科学技术开发、讲学、进修、培训、学术会议、文献资料交换、考察、谈判、合作研究、合作设计、合作调查、合作经营、展览、咨询等“因公”活动，以及旅行、探亲访友等“因私”活动。

在境内从事涉外活动，应当向所在单位报备，并接受保密提醒，签署保密承诺书。因公、因私出国（境），主要通过出国（境）证件集中统一管理、申报及领用前履行审批手续、行前保密教育、回国后及时回访等方式进行保密管理（参见图 5-2），并注意以下几点。

（1）核心涉密人员原则上不予批准因私出国（境），特殊情况应报国家国防科技工业局办理保密审批手续，教育部属高校的还应报教育部备案。

（2）因公出国（境）出访交流事项涉及国家安全、国家利益和重大社会利益的，出访前应当确定交流（谈判）保密方案与口径，经所在二级单位审核，报业务主管部门审批、保密管理办公室与国际处备案。

（3）特殊情况需携带涉密载体出国（境）的，应当按照相关规定由学校保密管理办公室报国家保密行政管理部门或学校业务主管部门报上级业

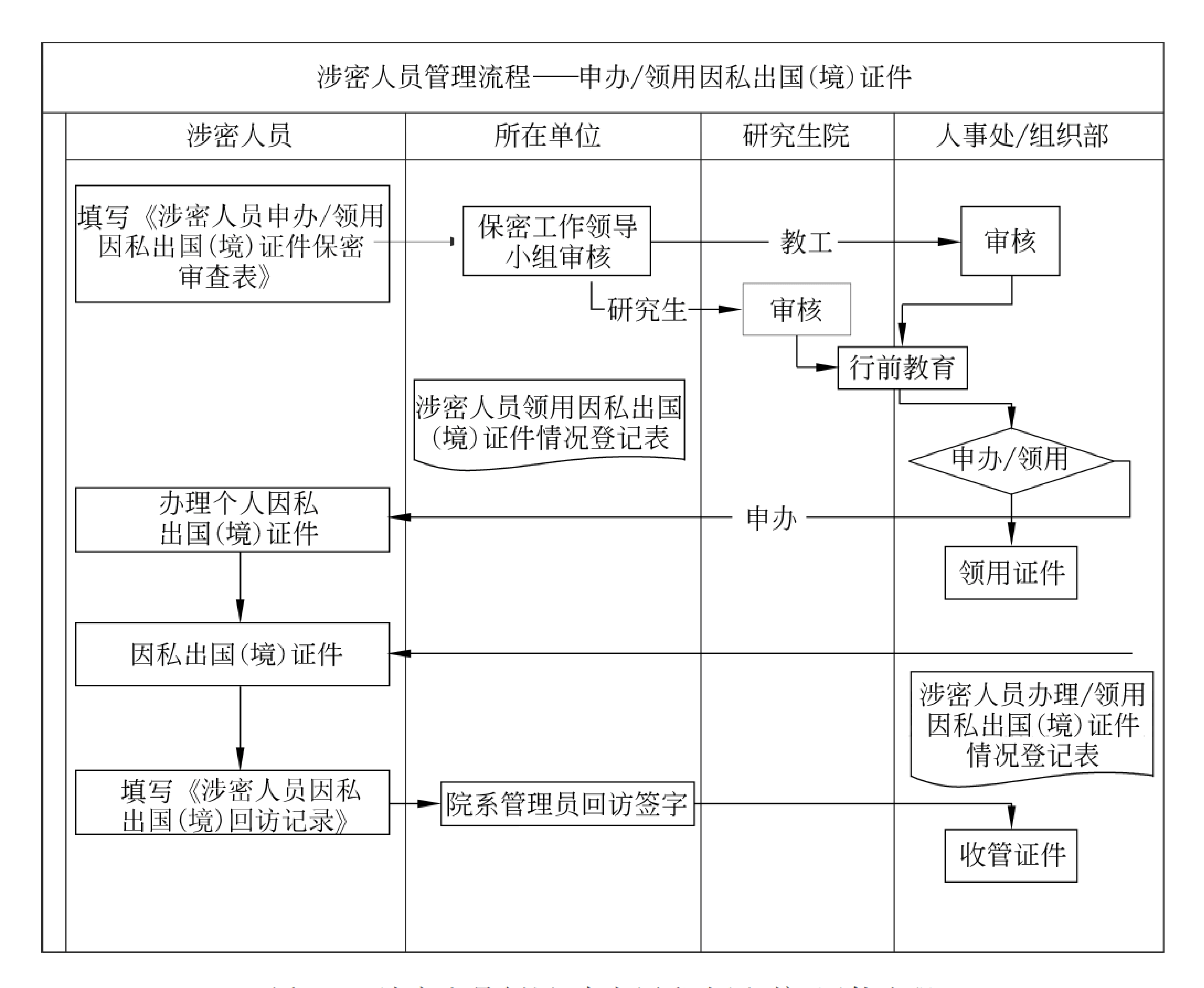


图 5-2　涉密人员领用/申办因私出国(境)证件流程

务履行审批手续,严格管理。

(4) 禁止将绝密级涉密载体携带出国(境)。

(5) 在国(境)外发现失泄密隐患或者发生失泄密情况应当立即向我国驻外使(领)馆以及学校保密管理办公室报告,并及时采取补救措施。

涉密人员发生下列情形之一的,所在单位及国际处等学校主管部门不得批准其出国(境)。

(1) 人民法院通知有未了结民事案件不能离境的。

(2) 发生泄密事件或有违反保密规定的行为正在接受调查处理的。

(3) 具有非法移民倾向的。

(4) 脱密期未满到国(境)外就业、定居的。

（5）出国（境）后可能对国家安全造成危害或对国家（或学校）利益造成重大损失的。

（6）其他法律法规和国家政策有明确禁止限制规定的。

涉密人员未经批准擅自出国（境），或出境逾期不归、叛逃，以及在境外遇到盘问、利诱、胁迫或其他重大异常情况的，所在单位知情后应及时向学校国际处、保密管理办公室、人事处进行报告，保密管理办公室及时上报国家有关部门，并采取必要的补救措施。

2. 保密补贴发放

发放保密补贴是强化涉密人员保密职责、增强保密观念、做好保密工作的一种补贴制度，对认真履行保密义务，遵守保密制度的涉密人员，按月足额发放保密补贴；对违反保密规定者，酌情部分或全部扣发保密补贴。保密补贴既可以由学校或基层单位统一支付，以体现学校或基层单位对保密工作的高度重视与条件保障，也可以从项目经费中列支，体现保密管理成本是项目管理成本中的一部分。各高校根据涉密人员涉密等级与单位经济情况自行确定补贴标准。保密补贴自涉密人员进入涉密岗位的当月开始发放，在其脱离涉密工作岗位并履行脱密手续的次月停发。

3. 涉密人员年度考核

每年年底，人事处应当组织对院系等二级单位的涉密人员遵守保密制度、履行保密职责等情况进行考核，同时要求涉密人员报告与境外人员通婚，接受境外机构、组织及其非亲属人员资助，本人或者直系亲属获得境外永久居留资格或者取得外国国籍等重大事项。对严重违反保密法律法规和保密制度，造成泄密事件或者酿成重大泄密隐患的，以及不再具备基本涉密资格的人员，应当及时调离涉密岗位。

4. 涉密人员资格复审

复审的目的是复核涉密人员国籍、政治立场、个人品行、学习经历、工作经历、现实表现、主要社会关系以及与国（境）外组织和人员交往情况等是否持续满足涉密岗位的要求，审查内容与上岗前保密审查内容一致。核心涉密人员每年复审一次，重要涉密人员每 3 年复审一次，一般涉密人员

每5年复审一次。

(六)离岗保密管理

涉密人员因涉密项目结题、工作岗位调整、借调到外单位、调出学校、退休等原因,脱离涉密岗位,应对其进行脱密期管理。

1. 脱密程序

涉密人员脱密流程参见图5-3。涉密人员提出脱密申请时(参见附表5-4),应当移交其保管和使用的全部涉密载体及信息设备(参见附表5-5),并承诺脱密期内继续履行保密责任。

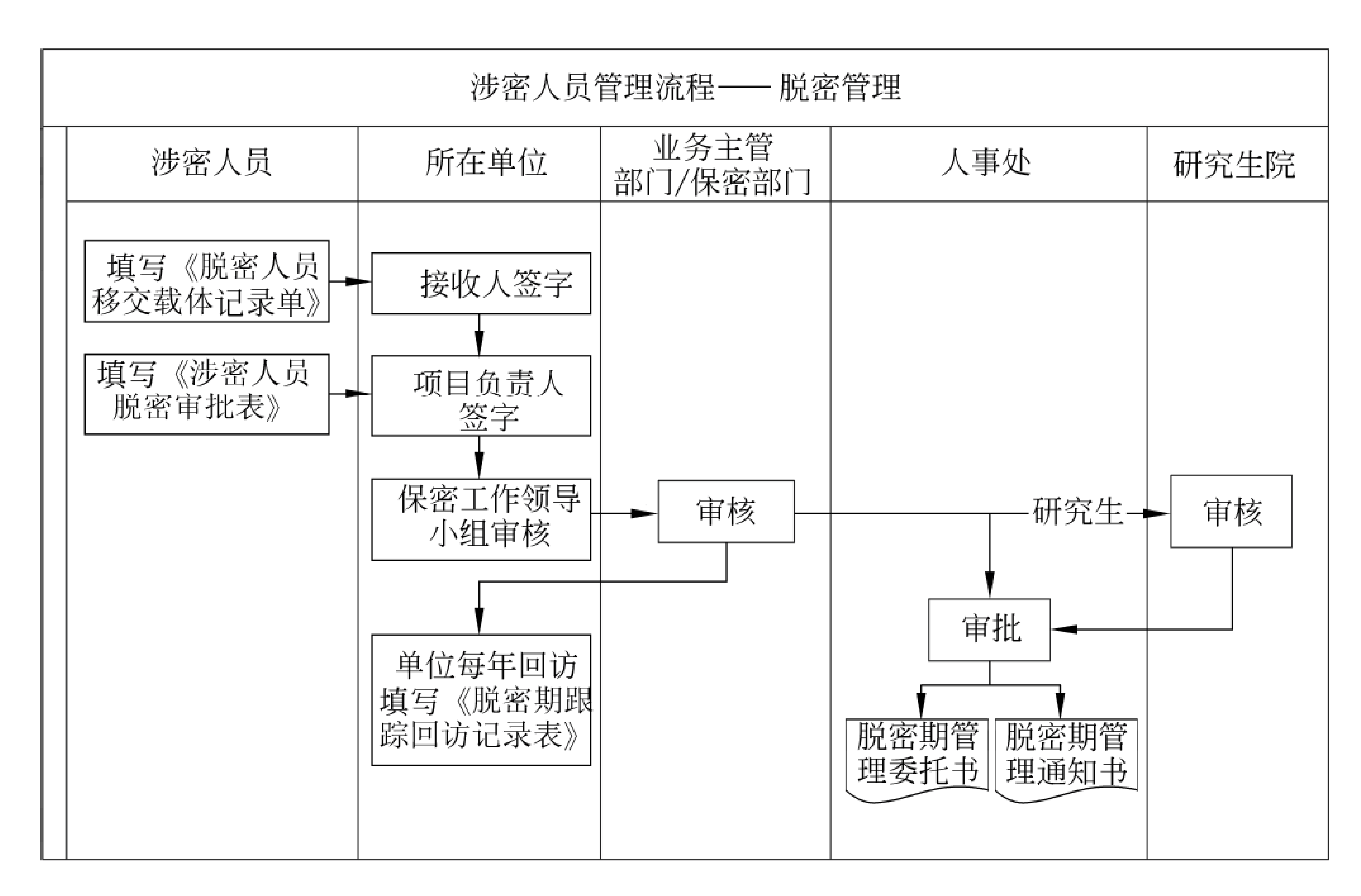


图5-3 涉密人员脱密管理流程

(1)不得到境外驻华机构、组织或外商独资企业工作。

(2)不得为国(境)外组织或人员提供劳务、咨询或其他服务。

(3)未经审批,禁止从事与原来涉密岗位相同的涉密业务活动。

(4)不得擅自出国(境)。

(5)在所掌握的涉密事项未解密前继续承担保密义务。

待其完成载体与设备移交，作出保密承诺后方可办理脱密手续。脱密期自其离开涉密岗位之日算起。核心涉密人员脱密期一般不少于3年，重要涉密人员脱密期一般不少于2年，一般涉密人员脱密期一般不少于1年。从事弹道导弹、核武器、军用核动力、核潜艇等装备研制的核心技术人员脱密期限不少于5年。

2. 脱密期管理

脱密期管理主要是指监管涉密人员脱密期内履行保密责任的情况，重点是对其涉外活动以及兼职情况进行监管。对在脱密期内的涉密人员，不得撤销其在公安机关出入境管理部门的备案，不得将出国（境）证件交给本人保管。

根据脱密人员去向，脱密期管理职责分工参考如下。

（1）继续在原单位工作或退休的涉密人员，由其所在二级单位负责其脱密期管理，由人事处向其所在单位发出脱密管理通知书。

（2）校内调动的，由接收单位负责其脱密期管理。人事处负责下达涉密人员脱密期管理通知书。

（3）调离学校、拟调往各级党政机关、国防企事业单位或其他以公有制经济为主体的企事业单位的，由接收单位履行脱密期管理，人事处负责将涉密人员脱密期管理委托书函告调入单位，并将涉密人员出国（境）证件移交调入单位。在确定调入单位为其在公安机关出入境管理部门备案前，学校不得撤销原有备案，直至脱密期结束。

（4）不属于上述情形的，人事处应当将涉密人员脱密期管理委托书函告其社保关系转入地的地市级以上保密行政管理部门。对社保关系转入地不明确的，应当将脱密期管理委托书函告其户籍所在地的地市级以上保密行政管理部门。

3. 脱密期回访

涉密人员脱密期内，脱密期管理单位每半年对其进行回访，了解脱密期内涉密人员工作、生活、履行保密责任等有关情况，重点是了解涉外活动以及兼职情况，并填写脱密期跟踪回访记录表。脱密期管理单位未落实

的，由调出单位对其进行回访。

三、各类科研人员保密管理

参与涉密科研工作的人员包括直接接触、处理项目涉密事项的涉密人员，也包括虽未直接参与涉密工作，但有机会间接接触涉密事项的课题组非涉密人员。科研人员的保密管理不仅要从整体上做好涉密科研人员的全过程管理，也需要对不同类型的科研人员，针对性开展保密管理，区分管理的重点和要点。

（一）涉密项目负责人

涉密项目负责人是涉密项目的第一责任人，也是涉密项目的保密工作负责人，对科研项目/课题组的保密工作承担直接管理责任，包括：知悉项目涉密事项，确定项目涉密岗位与涉密人员，严格控制知悉范围，提供项目/课题组开展涉密工作的保障条件，确保涉密项目全过程符合保密要求等。为了保证项目/课题组保密管理工作落到实处，项目负责人需要重点关注。

（1）做好项目产生的注意事项的密级、保密期限和知悉范围的拟定工作，严格按照工作需要控制注意事项的知悉范围。

（2）明确项目组成员保密职责，组织学习保密法律法规、规章制度及保密知识，提高保密意识和技能。

（3）指定专人负责项目组涉密载体管理，确保涉密载体安全。

（4）加强项目组信息设备和存储设备的保密管理，配备必要的安全保密设备。

（5）监督检查项目组保密工作落实情况，及时组织整改。

针对项目负责人的岗位职责，对项目负责人的管理要点主要包括以下几点：

（1）上岗前保密谈话，使其明晰涉密项目负责人岗位的保密责任和保

密工作重点。

（2）项目立项前，重点沟通确认项目涉密事项（含密级、保密期限和知悉范围）界定的符合性与准确性以及保密条件保障情况。

（3）结合项目执行过程的科研活动，对其进行保密检查。

（4）加强对其学术活动和对外交流的保密审查与提醒。

为了促进学科交叉发展，很多高校建立跨院系的科研机构，这就存在部分项目负责人在校内多个科研实体开展涉密科研工作的情况。比如有些教师既是某院系的教授，又是某科研机构的研究人员，其牵头承担的涉密项目可能依托不同的二级单位。对这类跨院系项目负责人的管理，一般应当按照“属地”管理原则，人员管理（如培训、对外交流等活动）由其人事关系所在单位负责，与科研项目保密管理工作（如项目执行过程中使用的信息设备、形成的涉密载体、召开的涉密会议等），应当由具体项目依托单位负责。

（二）涉密研究生

研究生是高校科研的重要力量，部分研究生因工作需要必须参与涉密科研项目接触涉密项。鉴于研究生思想活跃、交流愿望强烈、流动性强，管理过程中应当注意以下事项。

（1）指导教师或涉密项目负责人应当尽量选择留校或去国家机关、部队或国有大中型企业工作的研究生参与涉密工作，严格控制涉密研究生的数量和涉密等级，研究生一般只能接触、知悉、产生和处理秘密级国家秘密事项；

（2）参加校内涉密项目涉密工作的研究生，指导教师应当在论文开题前及时将其界定为涉密研究生，并纳入学校涉密人员管理范围。参加校外单位涉密工作的研究生，指导教师应与该单位共同协商确定其保密管理分工，并在双方保密管理机构备案；

（3）除参加学校、院系、研究生院、课题组组织的保密培训外，指导教师（或涉密项目负责人）应当对涉密研究生进行经常性保密教育，并将涉密项目研究内容分解后让研究生进入课题；

(4) 学校应当将研究生保密管理要求融入研究生培养的各个环节,开题报告、中期考核、最终学术报告、论文评审、答辩、学位审议等环节涉密的,涉密材料应当按照学校涉密载体保密相关规定进行管理,相关会议的组织应当执行学校涉密会议相关规定;

(5) 涉密研究生毕业离校前应当按照学校涉密人员管理相关规定履行脱密手续,所在院系对其进行保密教育谈话。脱密期内定期对其回访,掌握其去向。

(三) 参与涉密项目的非涉密人员

高校课题组参与涉密项目的非涉密人员有机会知悉涉密项目背景或涉密事项。项目负责人在项目讨论过程中除按照最小化原则严格控制涉密事项知密范围外,还应当经常对课题组全体人员进行保密教育和提醒,对课题组非涉密人员提出安全保密管理要求,严格控制研究内容和活动区域,离岗前签署保密承诺书。

1. 提出安全保密管理要求

主要包括:不在国际互联网计算机以及个人计算机、存储介质中处理、存储涉密项目内部信息;未经批准不将内部工作机带离工作场所;不以任何形式和途径主动探听、获取涉密项目有关涉密信息;不擅自披露涉密项目信息;学术论文投稿前,应当报项目负责人或导师进行保密审查;不得将个人计算机、移动存储介质等设备带入工作场所,不得私自将同学、同事、朋友等外来人员带入工作场所。

2. 严格控制研究内容和活动区域

项目负责人或导师应当对课题组非密人员可从事的科研项目研究内容、使用的载体、设备等作出限制,并划定其工作场所活动区域。有非密人员参加学术讨论时,应当回避项目相关涉密信息。

3. 课题结束或离校前移交涉密项目相关内部资料

课题组专兼职保密员应当对非密人员移交的载体和物品逐项逐件清点核对,履行签收手续,并对其带出资料、物品等进行保密检查。

4. 离岗前签署保密承诺书

承诺内容包括：对项目研制期间掌握、知悉的国家秘密和内部信息按规定时限承担保密责任；对外发表与涉密项目相关的论文、著述经项目负责人或导师保密审查通过方可投稿；自觉履行国家和学校保密要求，并接受监督；违反保密承诺，自愿承担法律责任等。

（四）国防领域专家

军委科技委或装备发展部等国防科技决策与国防科技计划实施管理部门根据国防科技发展需要，聘请很多国防领域专家，参与战略咨询、战略规划的研究和制定、涉密课题的评审和验收等工作。这些专家有不少来自高校，往往是各个科学技术领域的学术专家，取得较高的学术成就，具备较大的社会影响力。由于参与专家组活动，专家会掌握大量的国家核心技术与战略技术秘密，涉密事项范围广、涉密程度深，其接触的涉密事项范围已不限于学校产生、管理的涉密事项，因而，加强对国防领域专家的保密管理十分重要。这些专家一方面应当接受聘用机关、单位的保密管理，包括签署保密承诺书，参加专家组活动前接受保密提醒和教育，接受专家组保密检查等，还要按照学校的保密管理要求进行管理。

管理要点主要包括以下内容：

（1）推荐专家时，选择具备涉密资格的人员，并先行对其进行保密提醒、教育，包括聘用后可能接受的保密管理内容、承担的保密责任与义务等。

（2）获得批准后，应当及时根据专家组的要求，将其界定为相应涉密等级的涉密人员，并按照学校涉密人员的管理规范进行上岗、在岗、离岗全过程保密管理。

（3）及时跟进专家参与的专家组活动，并提供有针对性的保密管理服务，比如各类专家组活动主要失泄密风险点分析与应对措施建议，告知涉密会议与涉密载体的保密管理要求。

（4）定期组织专项检查，重点跟踪专家组资料的保密管理情况，同时检查专家及其团队信息设备的管理情况。

（5）对专家组尚未要求纳入涉密人员管理的专家，也要提出安全保密管理要求，组织签订保密承诺书。

（五）外协外包人员

外协外包人员是指承担学校涉密科研项目协作配套及为学校提供军工涉密业务咨询服务的校外单位的人员。

按照协作配套保密管理办法规定，应当选择具备相应保密资格的外协外包单位，并与外协外包单位签订保密协议，同时要对外协外包人员，特别是因工作需要到学校从事与协作配套任务或咨询服务相关的涉密工作的人员加强管理。主要包括：

1. 从事外协外包任务的部门和人员相对固定

要求外协外包单位指定相对固定的部门和人员负责学校军工涉密外协外包任务，参与外协外包涉密业务人员应当界定为外协外包单位的涉密人员，咨询服务单位委派的人员（包括外聘专家）还应当通过国防科工局组织的军工涉密业务咨询服务安全保密专项培训和考核，获得相应的培训证书。

2. 组织到学校从事涉密业务的外协外包人员签订保密承诺书

承诺内容包括：保守外协外包任务涉及的国家秘密和内部信息；严格遵守保密协议与学校的保密制度；自觉履行保密责任和义务，接受保密检查或审查；离岗后，在保密期限内继续对从事外协外包任中掌握、知悉的国家秘密承担保密责任；违反保密承诺，自愿承担法律责任等。

3. 对外协外包单位的涉密人员进行安全保密培训与检查

任务所属单位与校内项目负责人应当结合外协外包任务开展有针对的保密教育，并把外包外协人员纳入学校及任务所属单位保密检查范围和计划。

4. 严格限制涉密范围和活动区域

外协外包人员仅限于接触与涉密合同相关的涉密事项和涉密文件资料。校内项目负责人应当事先确定可供外协外包涉密人员使用的技术文件、图纸等。提供时，还应当隐去与外协外包任务无关的内容。同时，严格限制外协外包人员的活动区域，不得进入与外协外包任务无关的场所。

5. 任务完成后全部移交个人留存的涉密载体

外协外包任务结束前，外协外包单位与外协外包人员应当将学校提供给外协外包单位的，以及在学校从事外协外包任务时提供给外协外包人员的涉密文件资料、设备等悉数移交学校，并签订离岗保密承诺书。学校应当指定人员负责清点核对，确保准确无误。

（六）涉密场所工勤服务人员

高校涉密场所工勤服务人员是指因工作需要可能接触涉密信息的内勤安保服务等人员。工勤服务人员有机会出入涉密场所、接触涉密设备与载体，应当对其进行重点监管。

1. 上岗前政审及安全保密培训

学校聘用工勤服务人员，应当委托工勤服务公司或者组织保卫部对其个人及家庭情况进行背景审查。不得使用有犯罪记录的人员从事工勤服务工作。

工勤服务人员上岗前，聘用部门应当对其进行岗前安全保密培训并签订保密承诺书。培训内容包括：安全保密基本常识、工勤服务人员安全保密管理要求，发生泄密事件应承担的法律责任等。

2. 在岗期间保密管理

工勤服务人员在岗期间，使用单位应当对其经常进行安全保密教育，并明确专人管理，严格控制其活动区域，禁止工勤服务人员私自单独出入涉密场所。教育内容包括：安全保密提醒、安全保密具体要求、紧急情况处置等。同时，对其政治态度、思想状况、工作表现等情况进行定期考察。对存在不良倾向的，应当及时辞退，并报告保密管理办公室。

学校举办涉密活动需要工勤服务人员提供保障时，主办部门应当对其服务时限、区域、路径等提出明确要求，防止扩大涉密事项的知悉范围。

3. 离开服务单位签订保密承诺书

保密承诺内容包括：不得对外披露在学校工作期间所接触的涉密信息和内部信息；继续履行保守国家秘密的义务；违反保密承诺，需要承担相应法律责任等。

附表 5-1　培训效果评价表示例

培训效果评价表

单位：　　　　　　　　　　　　　　　　　　　　　　　　姓名：

<table>
<tr><td>组织部门</td><td></td><td>培训时间</td><td colspan="5">年　月　日</td></tr>
<tr><td>培训教师</td><td></td><td>培训内容</td><td colspan="5"></td></tr>
<tr><td colspan="2">课 程 内 容</td><td>非常好</td><td>很好</td><td>好</td><td>一般</td><td>差</td><td>很差</td></tr>
<tr><td colspan="2">课程主题是否切合工作重点、个人需要</td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td colspan="2">课程内容是否切合实际、便于应用</td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td colspan="2">课程知识是否深度适中、易于理解</td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td colspan="2">培训教师</td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td colspan="2">专业水平与课程准备充分程度</td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td colspan="2">表达清晰、态度友善</td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td colspan="2">互动良好，气氛活跃</td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td colspan="2">培训收获</td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td colspan="2">知悉保密形势，强化保密意识</td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td colspan="2">获得有效的知识或技能，利于后续工作</td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td colspan="2">哪些内容对你的帮助最大？</td><td colspan="6"></td></tr>
<tr><td colspan="8">整体上，您对这次课程的满意程度是：A. 不满 B. 普通 C. 满意 D. 非常满意
您给予这次培训的总评分是(以 100 分计)：________</td></tr>
<tr><td colspan="8">您认为课程或教师最应改进的地方？</td></tr>
<tr><td colspan="8">请您提出其他培训建议或培训需求</td></tr>
<tr><td colspan="8">备注：1. 填写完整后及时将本表交培训组织部门；
2. 请给予您真实的评估意见，以帮助我们不断提高培训水平。</td></tr>
</table>

附表 5-2　拟进入涉密岗位人员资格审查表示例

拟进入涉密岗位人员资格审查表

单位：

<table>
<tr><td>姓名</td><td></td><td>性别</td><td></td><td>民族</td><td></td><td>照片</td></tr>
<tr><td>出生年月</td><td></td><td>出生地</td><td></td><td>籍贯</td><td></td><td rowspan="3"></td></tr>
<tr><td>政治面貌</td><td></td><td>加入时间</td><td></td><td>国籍</td><td></td></tr>
<tr><td>文化程度</td><td></td><td>工作时间</td><td></td><td>学位</td><td></td></tr>
<tr><td>掌握语言</td><td></td><td>熟悉程度</td><td></td><td colspan="2">行政职务</td><td></td></tr>
<tr><td>技术职务</td><td colspan="3"></td><td colspan="2">公民身份证号码</td><td></td></tr>
<tr><td>户籍派出所</td><td colspan="2"></td><td>现家庭住址</td><td colspan="3"></td></tr>
<tr><td colspan="2">因公护照号码</td><td colspan="2"></td><td colspan="2">有效期起止时间</td><td></td></tr>
<tr><td colspan="2">因私护照号码</td><td colspan="2"></td><td colspan="2">有效期起止时间</td><td></td></tr>
<tr><td>人员类型
（√）</td><td colspan="4">事业编制人员（　），非事编人员（　），
博士后（　），研究生（　），其他______</td><td>教工号
/学号</td><td></td></tr>
<tr><td>拟进入涉密岗位</td><td colspan="6">□项目负责　□项目参与　□定密责任人　□科研管理　□保密管理
□人员管理　□载体管理　□设备管理　□财务管理　□其他____
____</td></tr>
</table>

工作经历（包括国内外经历）

起 止 年 月	工 作 单 位	岗 位

社会兼职情况

1. 是否在境外或其驻华机构兼职	是（　）否（　）
2. 是否为境外或其驻华机构提供各种咨询服务	是（　）否（　）

家庭及主要社会关系

身份号码	关系	姓名	性别	出生年月	国籍	工作单位及职务

续表

<table>
<tr><td colspan="3">本 人 承 诺</td></tr>
<tr><td colspan="3">以上情况属实。
本人签字：　　　　　年　　月　　日</td></tr>
<tr><td>所在单位人事审查意见</td><td colspan="2">以上情况属实。
主管领导签字：　　　年　　月　　日</td></tr>
<tr><td rowspan="8">所在单位党委审查意见</td><td>中华人民共和国国籍，无国（境）外永久居留权/长期居留许可</td><td>是（）否（）</td></tr>
<tr><td>与境外人员（含港澳台）无婚姻关系</td><td>是（）否（）</td></tr>
<tr><td>遵纪守法，无违法违纪劣迹</td><td>是（）否（）</td></tr>
<tr><td>作风正派，品行端正，无不良嗜好</td><td>是（）否（）</td></tr>
<tr><td>忠诚可靠，责任心和事业心强</td><td>是（）否（）</td></tr>
<tr><td>具有涉密岗位要求的工作素质和工作能力</td><td>是（）否（）</td></tr>
<tr><td>无其他可能影响国家安全利益的倾向</td><td>是（）否（）</td></tr>
<tr><td colspan="2">涉密资格政审：符合基本条件（　）　不符合基本条件（　）。
党委领导签字：　　　年　　月　　日</td></tr>
<tr><td>保密管理办公室审核意见</td><td colspan="2">已参加岗前保密培训，考试成绩合格。
负责人签字：　　　年　　月　　日
（单位盖章）</td></tr>
<tr><td>人事处审批意见</td><td colspan="2">负责人签字：　　　年　　月　　日
（盖章）</td></tr>
</table>

附表 5-3　涉密人员岗位密级审定表示例

涉密人员岗位密级审定表

<table>
<tr><td>姓名</td><td></td><td>性别</td><td></td><td>政治面貌</td><td colspan="3"></td></tr>
<tr><td>教工号</td><td></td><td>身份证号</td><td></td><td>从事专业</td><td colspan="3"></td></tr>
<tr><td>人员类型</td><td colspan="7">事业编制人员（　），非事编人员（　），博士后（　），其他＿＿＿＿＿＿</td></tr>
<tr><td rowspan="2">序号</td><td rowspan="2" colspan="4">涉密岗位名称</td><td colspan="3">密级（√）</td></tr>
<tr><td>秘密</td><td>机密</td><td>绝密</td></tr>
<tr><td></td><td colspan="4"></td><td></td><td></td><td></td></tr>
<tr><td></td><td colspan="4"></td><td></td><td></td><td></td></tr>
<tr><td></td><td colspan="4"></td><td></td><td></td><td></td></tr>
<tr><td colspan="8">以上情况属实。
项目负责人签字：
年　　月　　日</td></tr>
<tr><td>单位保密负责人意见</td><td colspan="7">建议该同志确定为（一般　重要　核心）涉密人员。
负责人签字（盖章）：
年　　月　　日</td></tr>
<tr><td>保密办审核意见</td><td colspan="7">1．该同志已签署保密承诺书（　）；
2．已谈话（对重要或核心涉密岗位的人员）（　）。
负责人签字（盖章）：
年　　月　　日</td></tr>
<tr><td>人事处审批意见</td><td colspan="7">负责人签字（盖章）：
年　　月　　日</td></tr>
</table>

附表 5-4　涉密人员脱密审批表示例

涉密人员脱密审批表

<table>
<tr><td>姓名</td><td></td><td>现所在单位</td><td></td><td>教工号</td><td></td></tr>
<tr><td colspan="2">原涉密岗位</td><td colspan="2"></td><td>原涉密等级</td><td></td></tr>
<tr><td colspan="2">原保密编号</td><td colspan="2"></td><td>联系方式</td><td></td></tr>
<tr><td>脱密原因</td><td colspan="5">1. 项目结题□
2. 岗位调整□　3. 离职□　4. 退休□　5. 借调、挂职□</td></tr>
<tr><td>脱密后去向</td><td colspan="5"></td></tr>
<tr><td>脱密期限</td><td colspan="5">自____年__月__日 至______年__月__日</td></tr>
<tr><td>涉密载体移交情况</td><td colspan="5">已办理移交手续，详见《脱密人员移交涉密载体记录单》</td></tr>
<tr><td colspan="6">保密教育提醒情况</td></tr>
<tr><td colspan="6">（本栏由负责保密提醒谈话工作的同志填写，脱密人员本人确认：）
1. 明确被谈话人的脱密期限和起止时间；
2. 告知负责脱密期管理的具体单位；
3. 告知不得违反规定出国（境），不为境外（驻华）机构、组织、人员及外商独资企业工作或提供劳务咨询等其他服务；
4. 重申在脱密期内有关管理要求；
5. 明确在脱密期内的重大事项报告程序。如，被谈话人在脱密期内，遭遇境外（驻华）组织、机构或个人利诱、胁迫、渗透、策反，本人及时向组织报告的有关程序。

教育提醒人签字：　　本人签字：
年　月　日</td></tr>
<tr><td colspan="3">以上情况属实。

项目负责人签字：
年　月　日</td><td colspan="3">单位保密负责人意见：

负责人签字（公章）：
年　月　日</td></tr>
<tr><td>校保密办审核意见</td><td colspan="2">负责人签字（公章）：
年　月　日</td><td>人事处审批意见</td><td colspan="2">负责人签字（公章）：
年　月　日</td></tr>
</table>

附表 5-5　涉密载体与信息设备清退交接登记表示例

涉密载体与信息设备清退交接登记表

<table>
<tr><td>姓 名</td><td></td><td>性别</td><td></td><td>涉密等级</td><td colspan="4">□核心　□重要　□一般</td></tr>
<tr><td rowspan="3">个人载体交接清退情况</td><td>纸质涉密载体</td><td colspan="3">名　称</td><td>密级</td><td>份数</td><td>页数</td><td>接收人或经管人核定后签名</td></tr>
<tr><td rowspan="2">电子涉密载体</td><td colspan="3">名　称</td><td>密级</td><td>份数</td><td>保密编号</td><td>接收人或经管人核定后签名</td></tr>
<tr><td colspan="3"></td><td></td><td></td><td></td><td></td></tr>
<tr><td rowspan="4">个人信息设备与存储设备交接清退情况</td><td>类别</td><td colspan="3">设备类型</td><td>密级</td><td>使用情况</td><td>保密编号</td><td>接收人或经管人核定后签名</td></tr>
<tr><td>涉密设备</td><td colspan="3"></td><td></td><td></td><td></td><td></td></tr>
<tr><td>存储设备</td><td colspan="3"></td><td></td><td></td><td></td><td></td></tr>
<tr><td>安全保密产品</td><td colspan="3"></td><td></td><td></td><td></td><td></td></tr>
<tr><td rowspan="2">场所出入权限回收情况</td><td rowspan="2">门禁卡、出入证、口令、权限信息</td><td colspan="6" rowspan="2">门禁卡、出入证____个，编号为：</td><td>经管人或负责人核定后签名</td></tr>
<tr><td></td></tr>
<tr><td>所属二级单位意见</td><td colspan="8">以上载体与信息设备交接手续齐备。
负责人签字：
（公章）　年　月　日</td></tr>
<tr><td>信息化管理部门意见</td><td colspan="8">已清点所列信息设备与存储设备，已对有关涉密信息进行了必要的清除。
操作人/负责人签字：
（公章）　年　月　日</td></tr>
</table>

第六章　涉密载体与密品管理

高校涉密科研工作是一项创造性的活动。在科研实践活动过程中，科研人员形成体现科研创新性的工作文件，研发出体现科研水平的设备与产品，这些载体和设备是知识和技术创新的重要工具和信息赖以附载的物质基础，往往直接含有国家秘密信息，或者通过观察、测试、分析手段能够获得其所承载的国家秘密信息。因此，涉密载体和密品的管理同样是保密监督管理的重点工作之一。

一、涉密载体管理一般要求

（一）定义与分类

涉密载体是指以纸、电、磁等为介质，以文字、数据、符号、图形、图像、声音等形式载有国家秘密的物件，包括载有国家秘密的文件、资料、论文、图表、书刊、软盘、光盘、移动硬盘、U 盘、磁带等。

根据载体介质的种类，涉密载体可以分为纸介质、光介质、电磁介质涉密载体等。

1. 纸介质涉密载体

纸介质涉密载体是指传统的机关单位在处理公务和进行科研活动中形成的含有国家秘密的纸质文件，包括文件、资料、书刊、图纸、电报、报表、会议材料、讲话稿、简报、研究报告、成果记录等。

2. 光介质涉密载体

光介质涉密载体是指利用激光原理读写涉密信息的存储介质，包括各

类光盘、光介质涉密载体。

3. 电磁介质涉密载体

电磁介质涉密载体是指利用电子原理和磁原理读写涉密信息的存储介质，包括各类U盘、移动硬盘等电子介质和磁硬盘、软磁盘、磁带等磁介质涉密载体。

（二）科研涉密载体范围

在高校涉密科研活动中，涉密载体的内容多种多样，可以是应用模型、学术论文、咨询报告、建议、方案、规划等，也可以是技术专利、计算机软件、程序或者是科研新理论、新方法及其科研设计、新产品的工艺流程、图表、数据等。

涉密科研项目产生的涉密载体范围主要包括以下内容：

1. 科研立项阶段产生的资料

如项目申请书、建议书、可行性论证报告、实施方案论证报告、开题报告、任务书、委托书、协议书、合同等。

2. 研究实施阶段产生的资料

如设计文件、图纸、实验报告、检验报告、重要的原始记录、项目进展报告、中期评估材料及重要的往来技术文件等。

3. 项目结题阶段产生的资料

如项目工作总结报告、技术总结报告、财务总结报告、成果测试报告、验收书、论文、专著、技术鉴定材料等。

4. 成果报奖阶段产生的资料

如成果和奖励申报审批材料、专利申请获奖、推广应用方案、总结、生产鉴定材料、推广应用的经济效益和社会效益证明材料等结论性材料。

5. 专项经费使用的相关证明材料

如专项经费支出合同审批表、协议书、合同、任务书、结题证明等。

6. 有关音像、照片等其他资料。

（三）管理职责分工

涉密载体应当按照其流转过程和业务分工实行分级管理。

1. 项目负责人

项目负责人是涉密项目保密管理的第一责任人，直接负责落实所承担项目规划建议、申报论证、立项、实施、验收和归档、鉴定报奖等全过程中涉密载体的保密管理工作。

为了确保科研项目涉密载体安全，同时又便利工作开展，一般应当以涉密项目组为单位对涉密载体实行集中管理，并在项目组内部指定专人负责本项目组涉密载体的日常保密管理。

2. 涉密院系

涉密院系作为涉密项目保密管理责任主体，应当对所有涉密科研项目组的涉密载体的制作、流转进行监管、审批，对台账汇总并定期清查核实。

3. 学校科研管理部门

学校科研管理部门作为涉密项目的业务主管部门，应当把涉密载体管理要求融入涉密项目管理的全过程中，在组织涉密文件查阅，接收、发放、报送涉密文件，以及组织涉密会议等过程中严格执行涉密载体管理办法。

4. 学校定点涉密复印室、机要收发室、档案馆、保密办、信息设备管理部门、保卫部等管理和保障服务部门

以上部门与学校涉密载体的制作、收发、保管、利用、维修和销毁等环节密切相关，在日常涉密载体流转过程中应当按照涉密载体管理办法实行监管。

（四）管理原则

涉密载体管理贯穿载体产生到消亡的全生命周期。涉密载体管理应当遵循“严格管理、严密防范、确保安全、方便工作”和“谁使用，谁负责”的原则，确保涉密载体全生命周期安全可追溯、可控制，做到：

（1）底数清楚：个人、二级单位分别建立涉密载体台账并定期核对；

（2）来源清楚：制作、收发、复制记录清晰，有据可查；

（3）去向清楚：借阅、传递、维修、销毁手续齐全，记录完整；

(4)集中输出:按学校、院系或课题组配备输出机,集中打印、刻录;

(5)集中复制:学校设定点复印室,凭审批复印;

(6)集中销毁:学校定期组织集中销毁。

(五)管理措施

为了减少在涉密载体制作过程存在的隐患和风险,可以采取以下管理措施:

1. 设置涉密载体集中输出点

对个人使用涉密计算机及外携笔记本电脑等采取关闭输出端口等技术措施控制涉密信息的输出,并在各单位、学校设置相对集中固定的涉密信息集中输出点,配备涉密输出机及专用存储介质,由专人操作和管理。参见图 6-1。

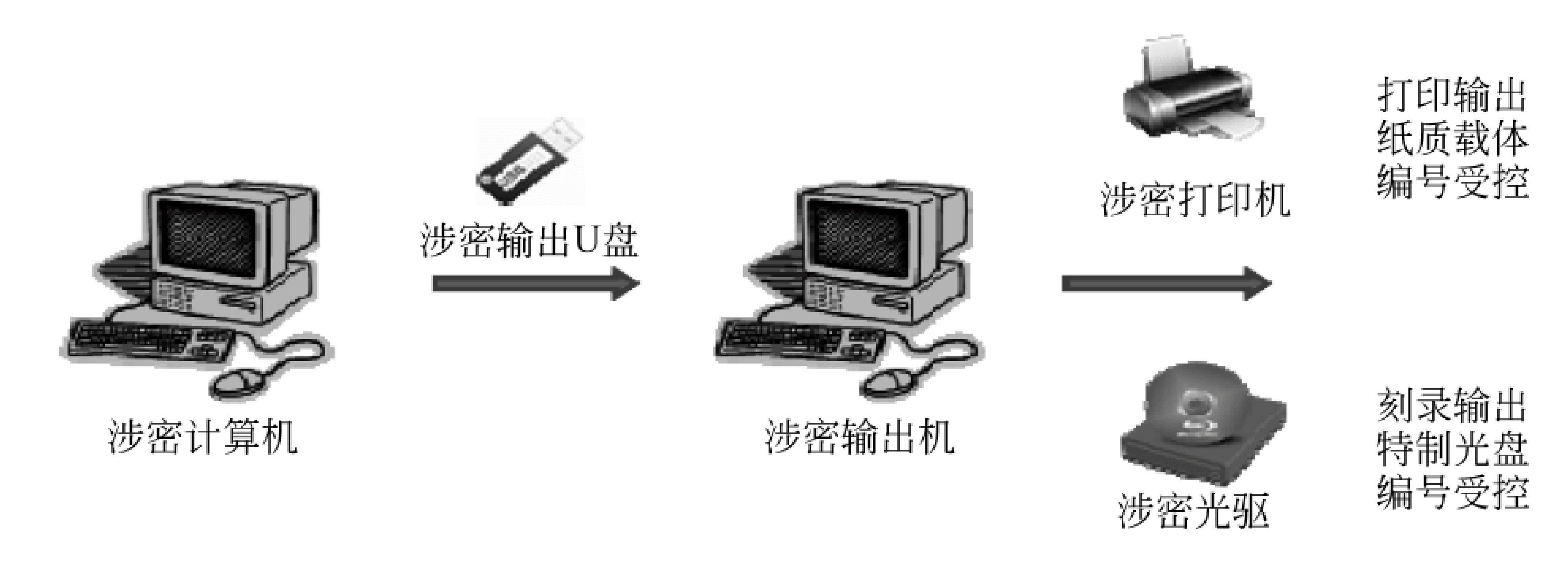


图 6-1 涉密载体集中输出示意图

2. 统一发放涉密载体受控章

为明显区分涉密载体,除了必须在载体的显著位置标识密级外,还可以统一加盖受控章(参见图 6-2)。对校内自制(含打印或复印),在制作完成后,由操作人员统一在载体封面加盖校内涉密载体受控章或复制涉密载体专用章;对涉密人员参加会议、观摩等活动带回的涉密载体,或通过机要渠道接收的涉密载体,应及时交给本单位保密管理员进行清点、核对,加盖受控章、编号登记后方可留存使用。

涉密载体受控章（**单位）			
编号		页数	
来源	□打印□接收	密级及期限	★
经办人		受控时间	年 月 日



涉密载体复印专用受控章 （复印地点）			
编号			
密级及期限	★	页数	
经办人		受控时间	年 月 日

图 6-2 涉密载体受控章、涉密载体复印专用受控章样式

3. 统一定制专用空白光盘用于制作涉密光盘

涉密信息设备导出涉密文件，应规范涉密光盘制作、标识及管理。如单位统一定制专用的空白光盘用于制作涉密光盘，能在一定程度上避免光盘无标识、不易区分的隐患。专用空白光盘应当由专人统一集中管理，涉密人员经单位负责人审批登记后领用，刻录完成后编号受控；损坏或其他原因不能使用的涉密光盘，不得随意丢弃或擅自销毁，须统一交回各单位保密管理员处留存备查，并按学校涉密载体管理要求集中销毁。

（六）涉密载体标识

涉密科研人员在科研活动中，应当对照科研项目立项时确定的涉密事项范围，对各阶段形成的包含国家秘密事项的文件、图纸、资料等涉密载体依照定密程序确定密级并准确标识。

涉密载体的标识为“密级★保密期限”，具体标识方法如下：

（1）纸介质形式的涉密载体，在封面或首页的左上角标明密级和期限。地图、图纸、图表等包含国家秘密的，在其标题之后或者下方标明密级和期限。

(2) 非纸介质形式的涉密载体应当以能够明显识别的方式标明密级和保密期限,凡有不可分离的包装(套、盒、袋等)的涉密载体,以恰当方式在其包装上标明密级。

(3) 计算机电子文档包含国家秘密的,在首页标明秘密标志,且与文档正文不可分离。

(4) 光盘、U 盘、移动硬盘、磁带等包含国家秘密的,在其正面标签的显著位置标明密级和期限。

(5) 文件、资料汇编中包含国家秘密的,分别标明秘密标志,并在封面或首页按照最高密级和最长保密期限进行标识。

(6) 摘录、引用属于国家秘密内容的涉密载体,以被摘录、引用的国家秘密中最高密级和最长保密期限进行标识。

二、涉密载体全过程管理

涉密载体的保密管理包括载体制作、收发、传递、使用、复制、保存、维修和销毁的全过程。在任何环节疏于管理都容易造成泄密隐患。

(一) 涉密载体产生过程

涉密纸介质和电子文档是国家秘密最常见的载体形式,其产生来源一般包括自制和外来两种。在学校单位或项目组内部制作产生涉密载体时应当准确标识密级,并编号受控,接收校外单位的涉密载体应及时受控并建立台账(参见图 6-3)。

1. 涉密载体制作

校内涉密载体的制作主要包括涉密计算机输出(打印涉密纸版文件或刻录涉密光盘)和涉密纸介质复印。

为了加强对涉密载体制作审批和受控的监管,方便科研人员制作符合科研活动要求的涉密载体,学校可以在各单位内部设置相对固定的涉密信息集中输出点,并创造条件设立集中的定点涉密复印室,提供专业的复印

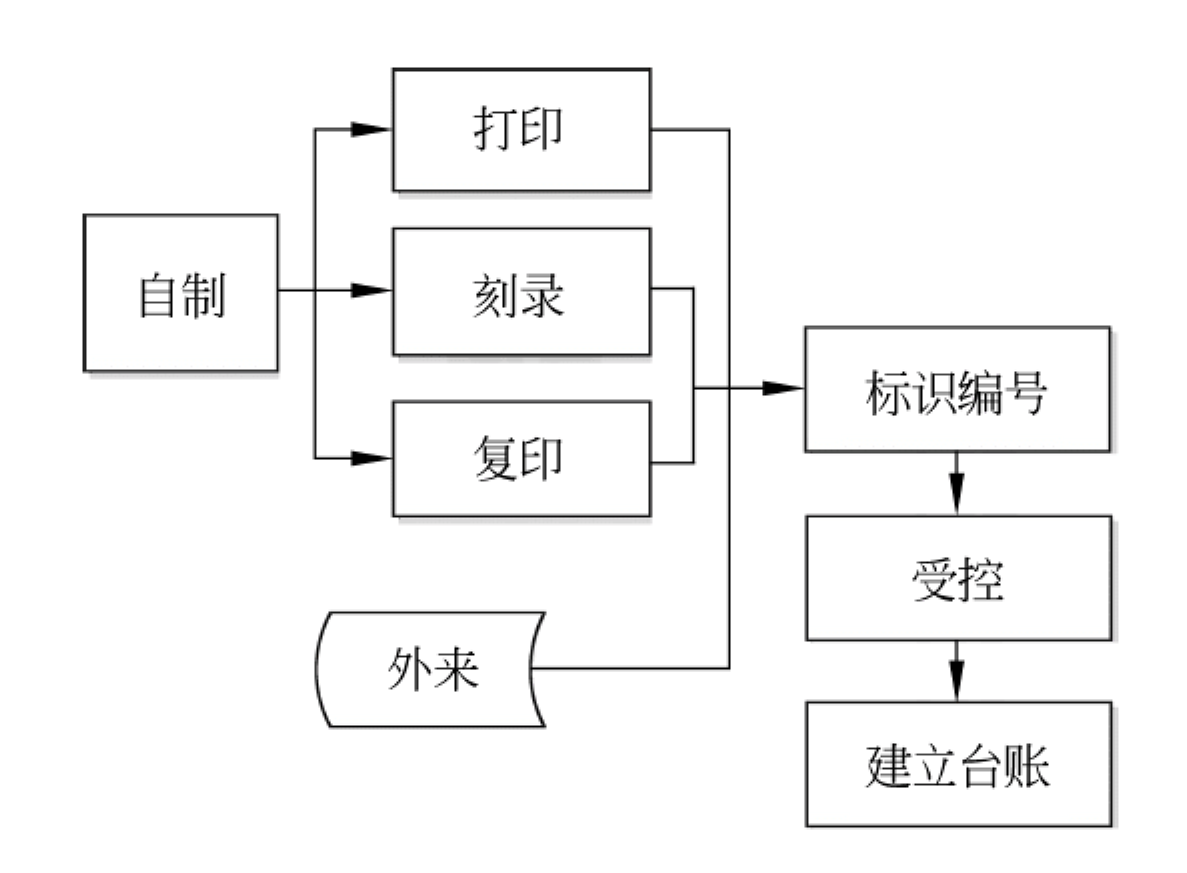


图 6-3　涉密载体受控过程示意图

装订服务。涉密输出机、复印机、载体受控章、特制专用光盘等由专人负责操作和管理。

打印与复印涉密载体应当履行制作审批手续(参见附表 6-1),确定制作的数量、发放和使用的范围等,经项目负责人或单位主管领导审批后,操作人员应严格按照批准的数量制作,在纸介质涉密载体首页盖上涉密载体受控章或复印专用章,刻录产生的涉密光盘应按照编号和密级准确标识。涉密载体制作过程示意图参见图 6-4,工作流程参见图 6-5。

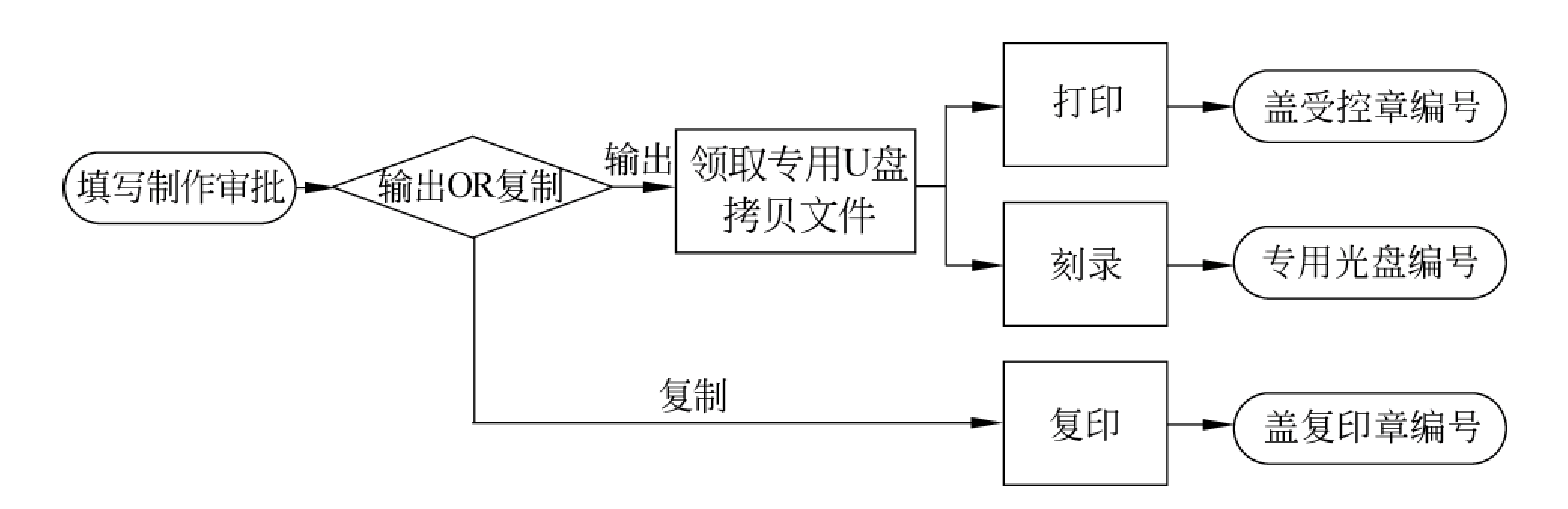


图 6-4　涉密载体制作过程示意图

对制作过程中产生的作废纸张、胶片、光盘等,为了保证与涉密计算机的输出审计记录保持一致,应当在审批表操作记录上准确登记,作废的纸张或光盘编号后留存,待统一销毁(参见图 6-6),不得随意抛弃或作为废品出售。

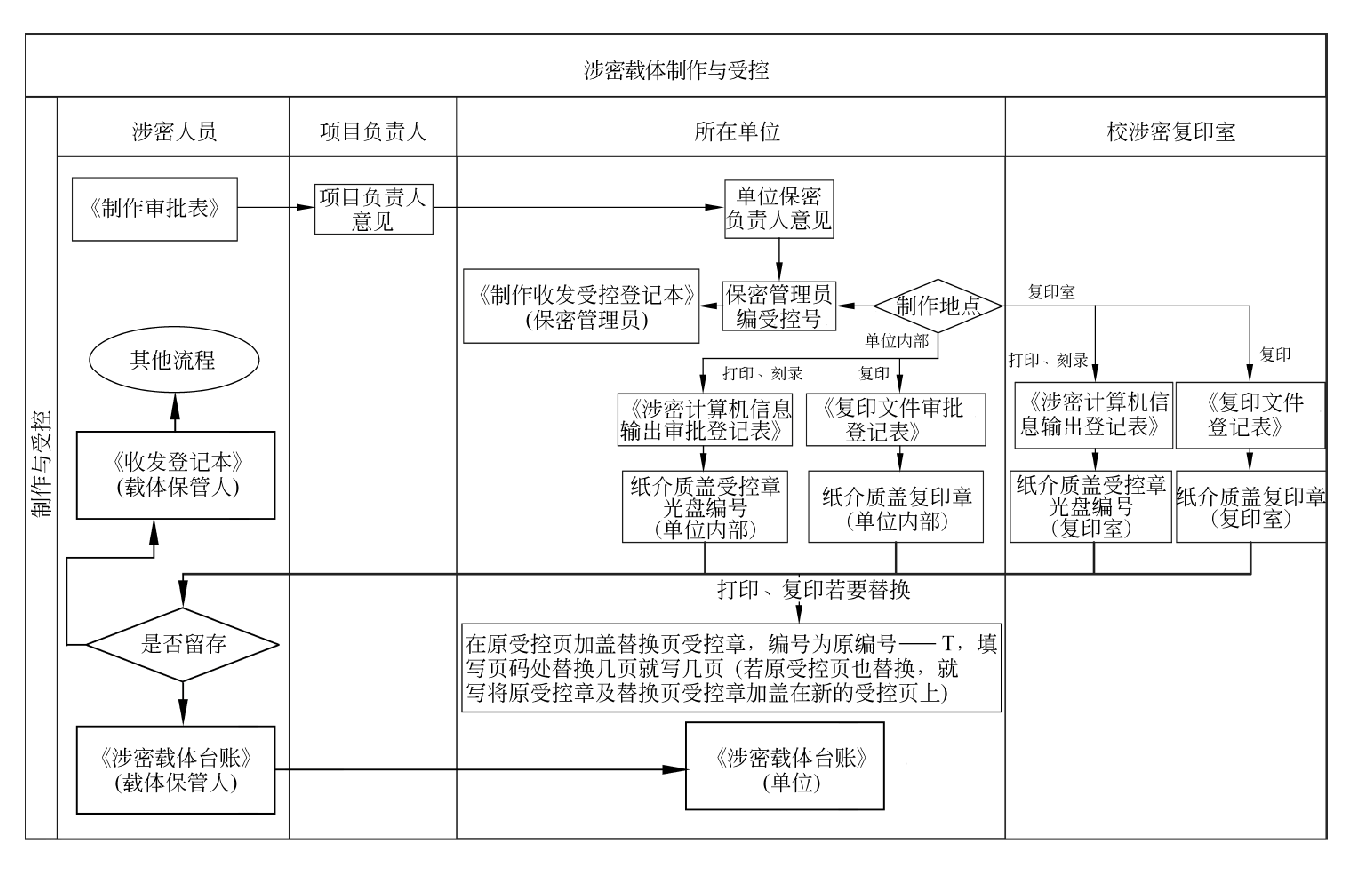


图 6-5　涉密载体制作工作流程

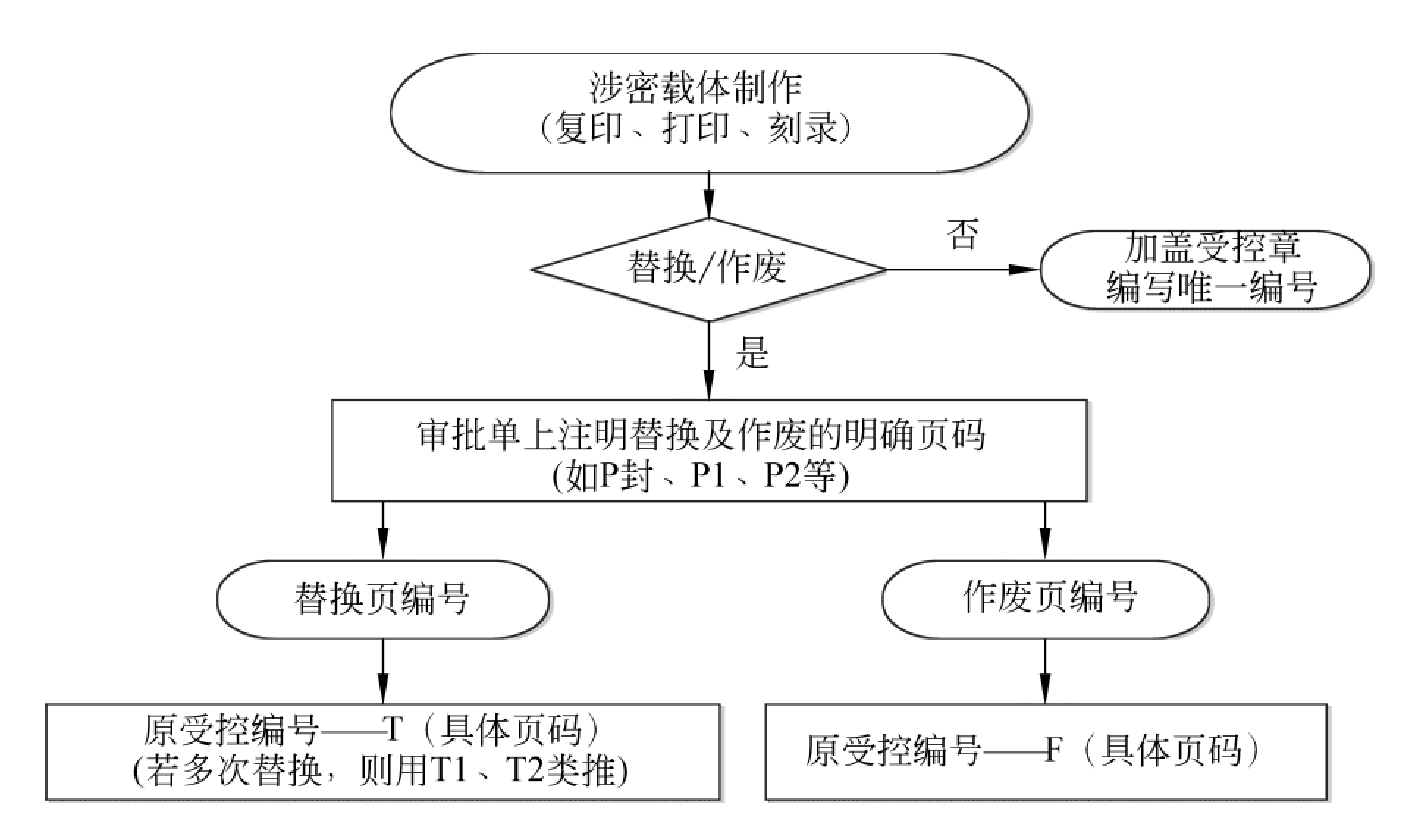


图 6-6　制作过程废页处理过程示意图

2. 涉密载体台账

为了保证涉密载体底数清楚，在涉密科研项目的研究过程中，科研人员根据工作需要制作、复制或接收技术报告、评估资料、总结报告等涉密载体时，应当首先交管理员加盖受控章、统一编号并登记（参见附表 6-2），确需留存的涉密载体，应当分别建立个人分台账和单位总台账（参见附表 6-3），并依据实际情况及时调整更新，做到账账相符、账实相符。流程参见图 6-7。

涉密载体台账的主要内容应包括：日期、载体类型、载体来源、载体名称或内容、密级及期限、载体编号、份数（或张数）、页数（或文件数）等。涉密科研人员个人保管的涉密载体类型主要是纸介质和光盘两大类，来源主要分为“自制”或“外来”，载体编号是产生或接收涉密载体时的校内受控编号。

涉密科研人员可以选择以电子版或手工填写的形式记录台账，并根据个人所保管涉密载体的流转情况实行动态管理，定期核查清理已经归档、解密、销毁的涉密载体。

项目所在单位应当定期对单位内部涉密科研人员的涉密载体管理情况进行检查核实，汇总单位内所有涉密载体总台账，做到账账相符。每年

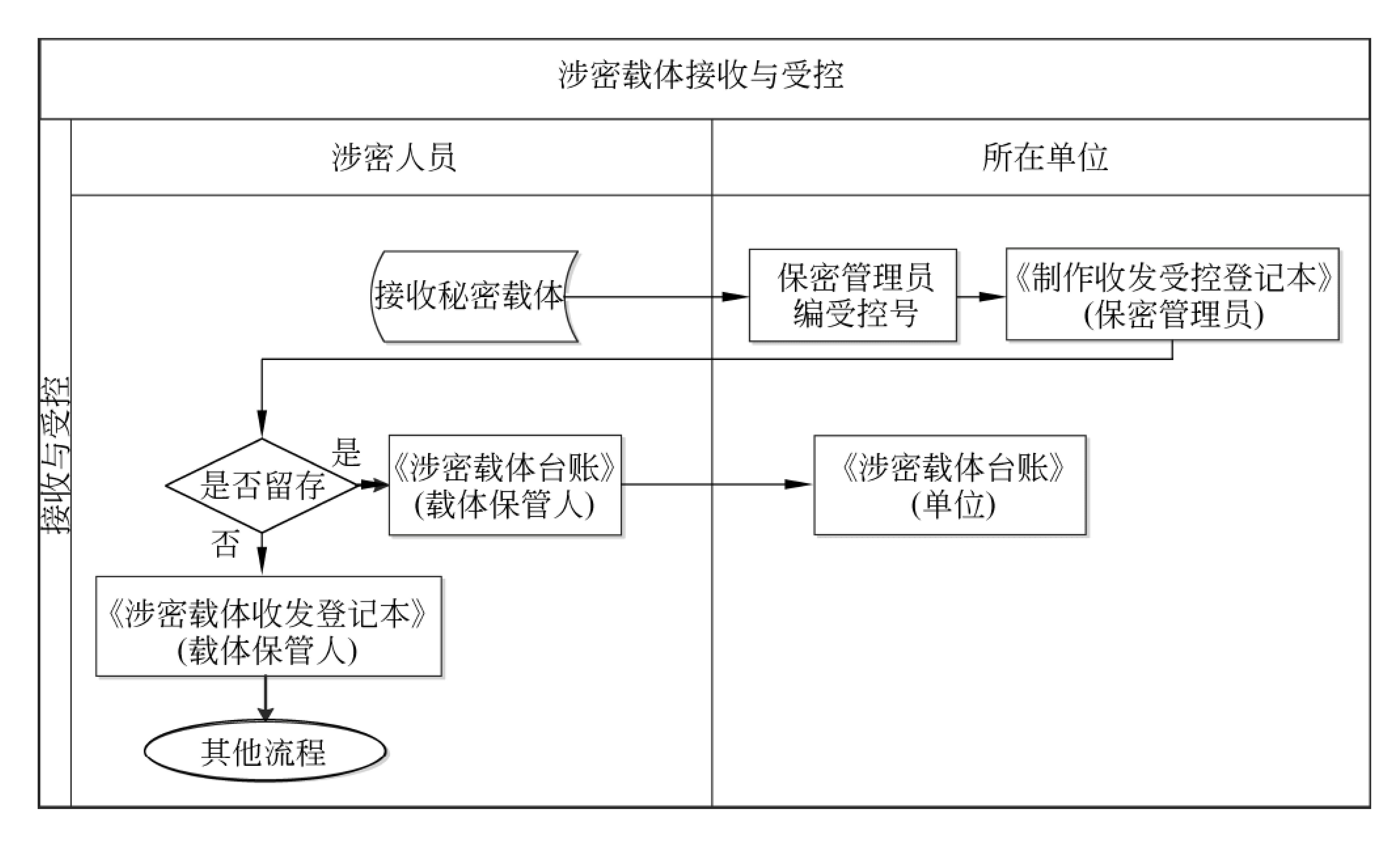


图 6-7　涉密载体接收工作流程

年度末对涉密载体按密级及类型的分类统计情况上报学校保密管理办公室备案。

（二）涉密载体流转过程

涉密载体流转包括在单位内部的涉密载体流转和校外的涉密载体传递处理。单位内部的载体流转一般是指校内单位及个人之间进行涉密载体的传递处理和载体移交。校外传递涉密载体应当通过机要交通、机要通信或指派专人进行，不得通过普通邮政、快递等无保密措施的渠道，禁止邮寄属于国家秘密的文件、资料和其他物品出境。

1. 涉密载体校内流转

对于一对一的涉密载体校内流转，一般可以在涉密载体收发登记本上记录流转过程(参见附表 6-4)。对于一对多或多对一的涉密载体集中发放或收集过程，例如科研管理部门组织涉密人员申报项目、领取指南，或涉密科研人员向科研管理部门提交项目申请书、建议书、论证报告、评审材料、总结报告时，载体的校内流转过程可以用涉密载体处理记录单记录(参见

附表 6-5),这种相对集中的涉密载体处理方式,既遵循科研活动的规律,又能简化工作流程。

2. 涉密档案归档

科研活动是一个不断创新的过程,在实践过程中积累的事实、数据、成功和失败的经验,记载和反映科研全过程和具体成果的文件材料及原始记录,以及研究人员撰写的以技术成果和科学理论为主要内容的学术论文、论著等,都是极有价值的科研档案,也是重要的信息资源和国家的宝贵财富,应当注意定期收集整理,到档案管理部门立卷归档、集中管理,并保证其连贯、完整和系统。涉密科研项目结题后,应当按照规定做好涉密科研档案的归档工作。

在涉密科研项目结题时,科研管理部门应当及时组织涉密项目资料归档工作(参见图 6-8)。项目负责人按照学校科研项目立卷归档的规定,指定专人负责科研项目各阶段的资料收集、整理、立卷和档案移交等工作。需要注意的是,立卷归档的科研档案资料卷宗封面或者首页的密级应当与卷内密件的最高密级和最长保密期限保持一致。

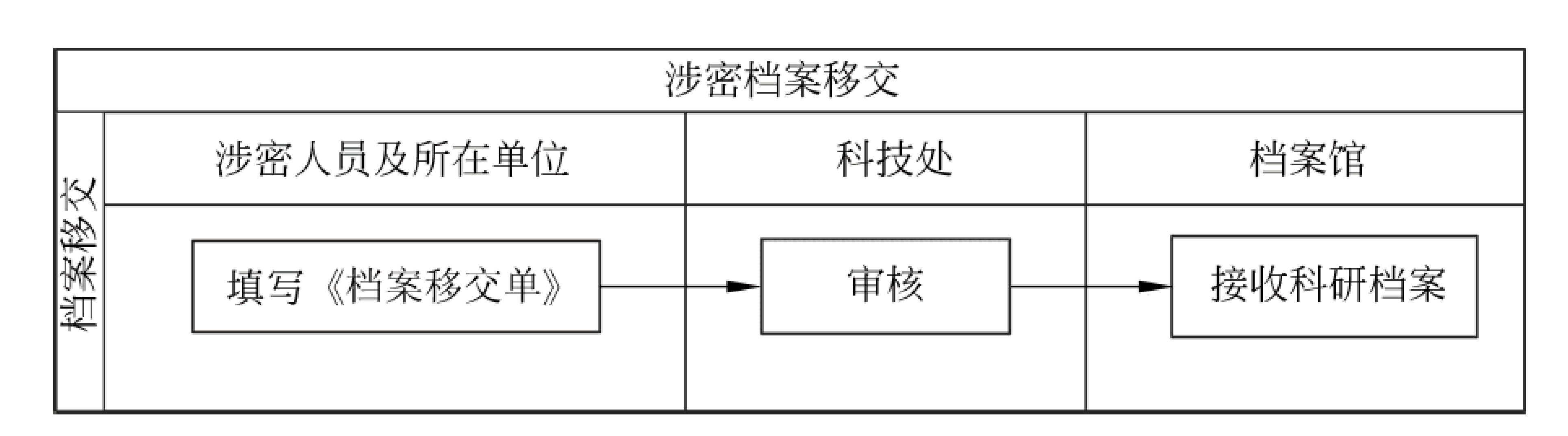


图 6-8　涉密档案移交流程

3. 脱密人员载体移交

涉密人员因涉密项目结题、工作岗位调整、借调到外单位、调出学校、退休、毕业等原因离岗离职前,应当全部清退其保管和使用的涉密载体,做好清点、核查工作,办理涉密载体移交手续,由所在项目组或单位指定专人接收移交的涉密载体。

4. 机要文件收发

机要文件管理包括机要文件的收发、传递、批办、阅读、保管、清退和销

毁等一系列工作。通过机要交通或机要通信部门送达的密件，应当由各单位机要文件管理人员接收并及时处理，其中注明“＊＊亲启”字样的密件要交给指定人员处理。不能及时交付或领取的密件，应由机要文件管理人员存放在有安全保障的专用场所或保密柜中。因故确需委托他人代领、代收文件的，应当出具书面授权书，被授权人代领、代收时应当提交书面授权书并签署保密承诺书。

各单位机要文件管理人员接收涉密载体时，应当对以下信息核对无误后方可履行签收手续。

（1）检查信封、包装、密封标志是否完好无损，确认未被拆开和漏失，发现问题应及时报告单位主管领导和发文单位处理。

（2）检查核对密件包装上的收文单位是否是本单位或所属部门，不属本单位的，应当立即退回机要收发员处理。

（3）拆封取出密件后要检查密件包装内是否有遗留的密件，检查签收单登记的文件名称和数量与所接收到的密件实物是否相符，如果不符，不能接收，并及时与发文单位联系核实，如果密件包装内有同时寄来的发文通知单，应当妥善保留备查。

机要文件管理人员应当详细登记所接收的密件的机要号、来文日期、来文单位、文件名称、发文字号、密级、份数、页数等信息并进行编号，加盖收文专用章，同时保存收发登记表备查（参见附表 6-6）。

机要文件管理人员在分发处理密件时，应当制作机要文件办理单，及时报主管领导阅批，并按照批示组织好密件的传递或传阅工作，不得自行扩大知悉范围，原则上应于接收密件当天，根据主管领导阅批意见，通知相关单位领取密件，或通知相关人员到指定场所阅读；需要传阅或复制下发的密件在处理时还应当填写机要文件分发处理记录单，内容包括文件来源、来文编号、文件资料标题名称或简要内容、密级及保密期限、分发受控编号、份数、发放范围等。

5. 机要文件发送

通过机要方式寄送文件时，应当履行机要发送审批手续（参见附表 6-7）。

同时，寄送人应当使用专用机要信封包装并在信封上标明密级和收发件单位名称。各二级单位机要文件管理人员登记后密封，并在信封封口处盖单位骑缝章。学校机要收发室指定专人负责涉密机要文件的收发工作，履行登记、签收手续，防止错发或漏发。机要文件发送流程参见图 6-9。

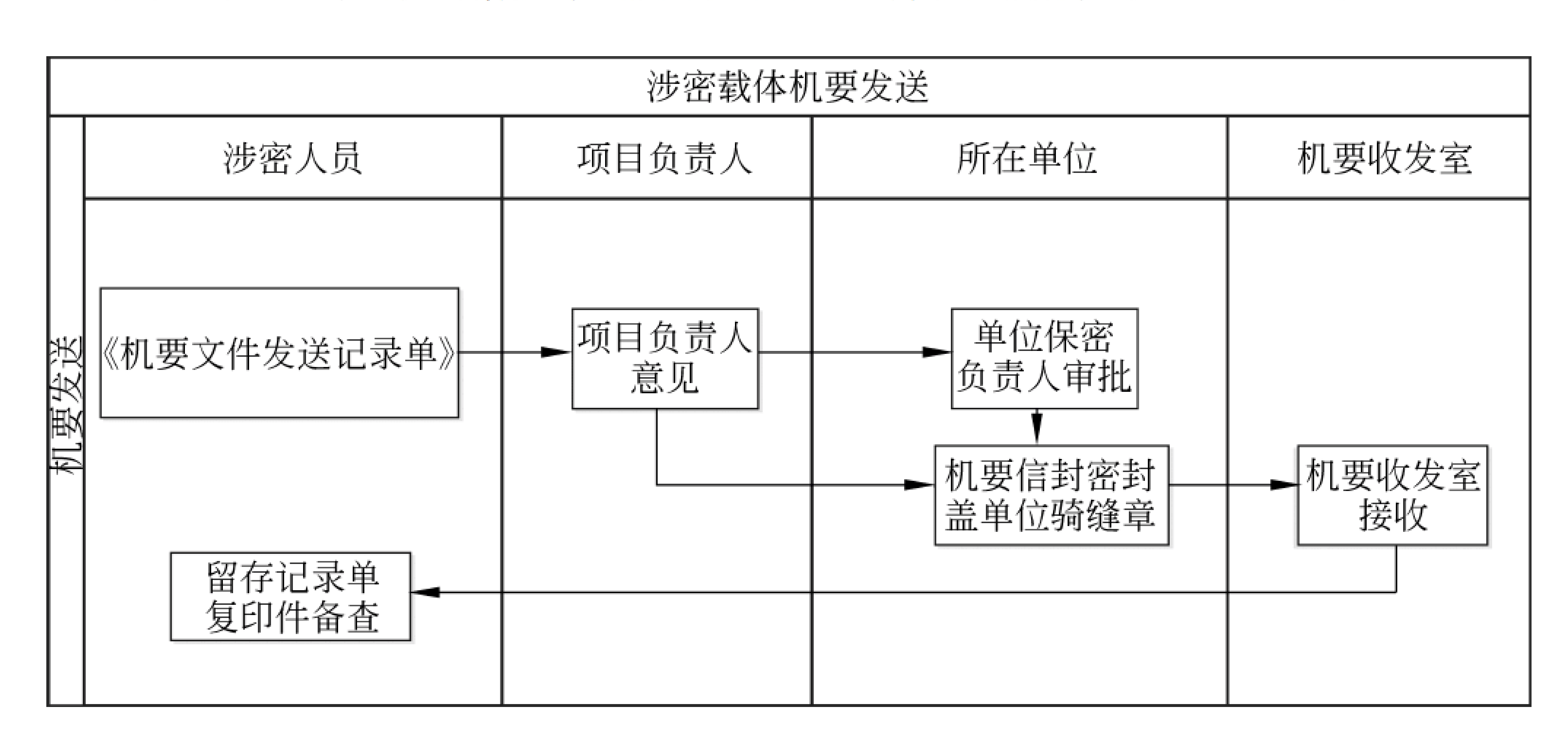


图 6-9　涉密载体机要发送工作流程

6. 校外专人传递

与校外单位的涉密载体收发和传递，除了通过机要交通或机要通信部门收发外，也可以在涉密人员参加科研活动时以专人送取的方式进行。

涉密人员携带涉密载体参加在校外组织的项目论证、评估、检查、评审、答辩、结题验收、成果鉴定等科研活动时，须履行审批手续(参见附表 6-8)，并详细记录涉密材料的使用、签收和带回情况。活动结束返回后，应当根据工作需要及时处理带回的涉密资料：需要在项目组留存继续使用的涉密载体应当建立台账，无须留存的涉密载体应当及时履行销毁审批手续，并妥善保存至学校组织实施集中销毁。校外专人传递工作流程参见图 6-10。

（三）涉密载体使用过程

科研项目的研究是一种阶段连续性的过程，涉密资料保存和使用也伴随各种科研活动贯穿于整个项目的全周期。涉密载体的使用包括涉密文

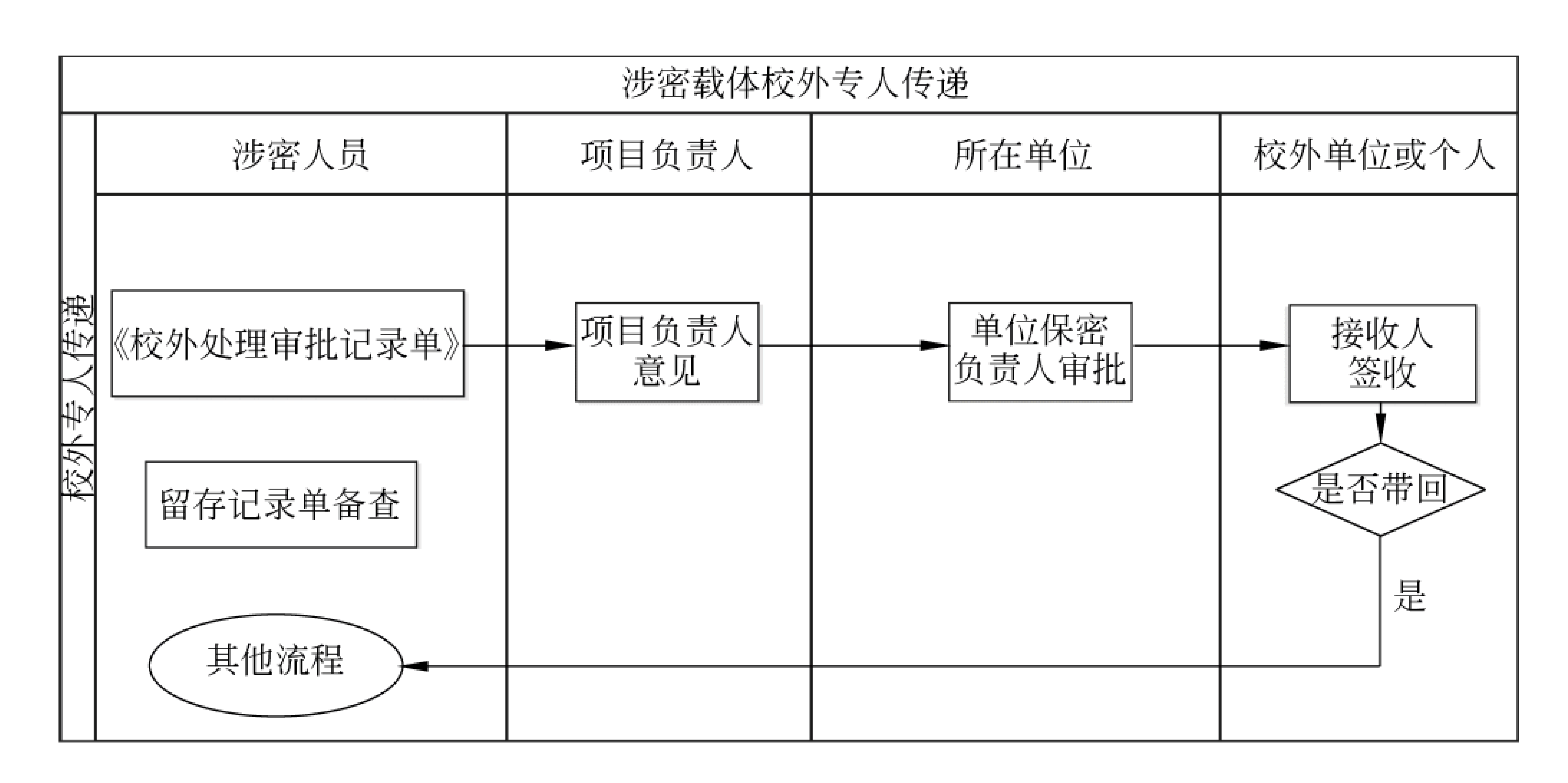


图 6-10　涉密载体校外专人传递工作流程

件资料的传达、阅读、借用、汇编、摘录及科研归档材料的利用等，每一个环节都应当遵照保密要求严格管理。

1. 涉密载体保存

保存涉密载体应当选择安全保密的场所和部位，并配备必要的保密设施、设备，实行集中、专人管理。秘密级和机密级涉密载体应当存放在密码文件柜内；绝密级涉密载体应当存放在密码保险柜内，钥匙和密码由两人分开管理。

科研工作人员离开办公场所，应当将涉密载体存放在机要室、档案室、资料室或课题组的资料保密柜内，不得将涉密载体随意存放在玻璃书柜和木质书柜中。涉密展板、密品等无法存放在保密柜中的涉密载体，项目组应当制定专门方案，将展板或密品集中存放在安装有安全设施的封闭场所内，并指定专人管理，确保知悉范围可控。

涉密载体管理人员应对所保管的涉密载体数量、密级、保密期限与知悉范围等做到底数清楚、记录清晰，定期清查、核对并及时追回应清退归还的涉密载体。

2. 涉密载体使用

使用涉密载体需要遵守以下原则。

（1）应当在符合保密要求的办公场所或指定地点使用，不得随意扩大涉密载体的知悉范围。

（2）传阅涉密载体，应当由经办人填写传阅卡，专夹传阅，记载密件份数、编号和阅读时间，阅读者之间不得横传，不得随意抄录密件内容，更不能私自复印。

（3）借阅涉密载体，应当办理登记、签收手续，对使用人、借阅时间、使用目的等做出明确记载，并限定归还的具体时间。归还所借密件时，要当面清点，办理退还手续。

（4）绝密级国家秘密载体不得外借，必须在管理人员指定的场所阅读，并对接触和知悉绝密级涉密载体内容的人员作出文字记载。

（5）汇编、摘录、引用涉密文件资料时，应当经原制发单位批准同意，形成的国家秘密载体，应当按其中的最高密级和最长保密期限标识和管理。

（6）不得携带涉密载体旅游、探亲、访友和出入娱乐场。

（7）不得擅自携带涉密载体参加涉外活动。确因工作需要携带的，必须履行审批手续，并采取严格的安全保密措施。严禁携带绝密级秘密载体参加涉外活动。

（8）不得擅自将国家秘密载体携带或邮寄出境，确因工作需要携带的，须履行审批手续，向地（市）级保密行政管理部门申办“国家秘密载体出境许可证”。严禁将绝密级国家秘密载体携带或邮寄出境。

3. 涉密档案利用

科研项目资料归档的最终目的是利用。为了国家秘密安全和科研成果发明人的专利技术秘密等知识产权保护，应当加强涉密科研档案的管理，做到利用有规定，管理有措施。查阅已归档的涉密科研档案，应当填写涉密档案利用申请表（参见附表 6-10），经档案负责人（一般为项目负责人）同意及所在单位保密负责人审批后，到学校涉密科研档案管理部门借阅。借阅涉密档案不得擅自留存、抄录和复印。

（四）涉密载体销毁过程

由于涉密载体承载国家秘密信息，退出使用、报废的光盘、U 盘、硬盘

和办公自动化设备的存储部件等涉密电子存储介质，以及无保留价值的纸介质涉密载体，应当实行集中销毁，不得随意转赠、转作他用或作为废品出售或丢弃，不得擅自销毁。

涉密载体销毁应当履行销毁程序（参见图 6-11），认真清点、登记，报单位保密负责人审核批准，销毁绝密级国家秘密载体还须报请制发单位批准（参见附表 6-11）。

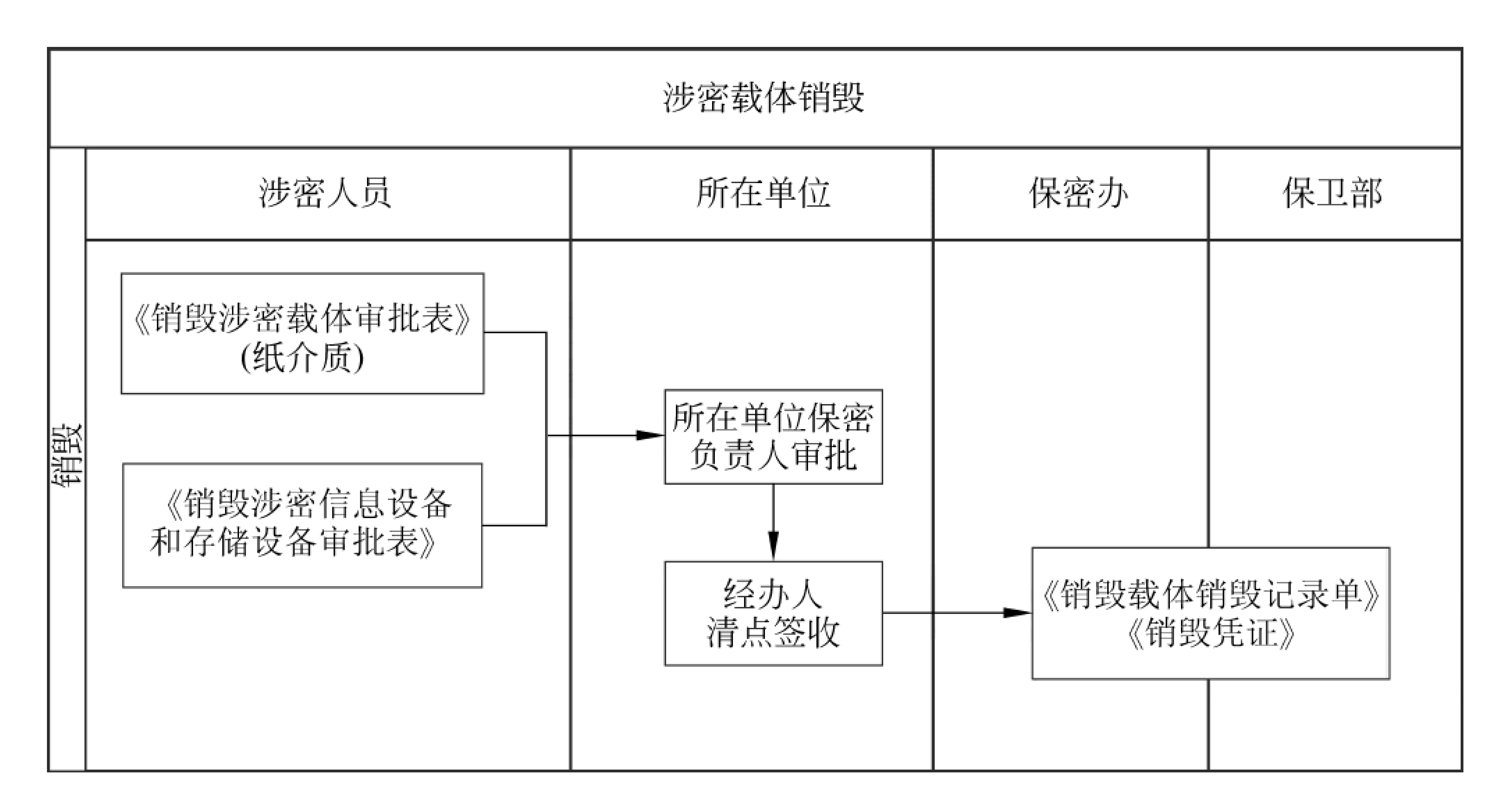


图 6-11　涉密载体销毁流程

批准销毁的涉密载体应当送交专门的涉密载体销毁机构或保密行政管理部门指定的承销单位销毁。因特殊原因不能及时销毁的，应当按保密管理规定进行保管，存放在符合安全保密要求的专门场所，不得随意搁置、堆放，不得私自留用。

送销涉密载体应当按照涉密载体类别分类封装，安全运送，并派专人现场监销，留存销毁记录（参见附表 6-12）。销毁纸介质涉密载体应当确保秘密信息无法还原，磁介质、光盘等应当采用物理（如消磁、粉碎处理）或化学的方法彻底销毁。为了防止涉密存储介质在报废销毁过程中发生失泄密，还应当在送销前使用具有保密资质的数据擦除处理或消磁设备进行处理。

（五）新型介质涉密载体

随着信息化的快速发展，信息处理也越来越依赖于各类电磁介质和光介质载体。除了传统的纸介质涉密载体外，大量承载涉密信息的磁盘、U盘、光盘为主的光、电磁介质等新型涉密载体已成为主流。根据定义，用于信息存储和交换的可读写装置如软盘、光盘、U 盘、移动硬盘、磁带、MP3、MP4 播放器、录音笔、数码相机存储卡等，都应当视为存储介质。这些新型载体的普遍应用，在为办公自动化带来方便的同时，也使得失泄密的风险随之加大。相对于传统的涉密纸介质载体，针对此类新型介质涉密载体的管理更为复杂，不可避免地成为涉密载体保密管理的重点和难点。

对光介质、电磁介质等用作涉密载体的新型介质，如移动硬盘、U 盘、存储卡等可以采取统一购买或统一标识等方式来加强其保密管理；通过技术手段对涉密介质进行注册授权和身份鉴别认证控制数据接口和信息导入导出；对涉密介质存储的涉密信息进行加密处理，防止违规交叉使用涉密介质或因涉密介质丢失而造成失泄密隐患；存储国家秘密信息的存储介质，应当按照所存储信息的最高密级进行密级标识；涉密存储介质还应当存放在保密柜或保险柜中，与非涉密存储介质分区保密。

涉密存储介质的维修，是保密管理的薄弱环节，应当采取管理措施，确保其所存储的国家秘密信息不被泄露。涉密存储介质维修一般由本单位技术人员负责，确需校外单位维修的，应选择有资质的定点单位。定点单位的专业技术人员上门维修时，应派专人在现场陪同，必要时可送交保密工作部门指定的定点单位进行维修或拆除信息存储部件或信息擦除后外送维修。

三、密 品 管 理

国家秘密设备、产品（以下统称密品），是指直接含有国家秘密信息，或者通过观察、测试、分析手段能够获得其所承载的国家秘密信息的设备或产品。通常是指具有重要国防意义的军事装备、产品、技术侦察设备，具有

国际领先技术水平且需要保密的科学技术设备、产品等。

密品的保密管理包括研制、生产、试验、运输、使用、保存、维修和销毁各环节的保密管理。管理对象既包括项目来源或合作单位提供的密品，也包括本单位科研过程中形成的密品。

（一）密品的标识和台账

密品研制、生产任务下达时，应当履行定密审批手续，确定密品的密级、保密期限，并明确密品的保密要点。密品应当以能够明显识别的方式在密品及其包装上标明密级、保密期限，并在有关技术文件中注明。

承担涉密科研任务的项目组及所在单位，应当指定专人负责密品的日常保密管理工作，确保各个环节记录清晰完备。经批准管理、使用密品的人员，对密品的安全负有直接责任。

研制、生产、购买或获得的密品，应当由各单位保密管理人员统一编号，保密管理员和密品保管人分别建立台账，对密品的密级、保密期限、保密要点、责任人等信息进行登记。做到账账相符、账实相符，并定期清查核对更新。密品保管人调离岗位时，应当对所管理的密品及其管理记录办理清点、移交手续。

（二）密品的研制、生产与试验

密品的研制、生产、试验场所应当符合保密要求，并加强安全防护措施，无关人员不得随意进入。外形或者构造易暴露国家秘密的密品，不得露天生产、保存、放置。因特殊原因需要露天放置时，应当采取必要的遮盖或其他保护性措施。有特殊要求的密品，应当对可能反映或者暴露其国家秘密的文字标志、特征标志采取伪装或删除措施。

绝密级密品的研制、生产应当在封闭场所进行，并设立专门的放置、保存场所，由专人负责保密工作，保证密品的安全。

密品的研制、生产、试验需要两个以上单位共同完成的，应当明确各自责任，确保密品在各个环节均受到严密保护，并严格控制和缩小知悉接触

范围;确需接触的,应当按有关规定履行报批手续。严禁无关人员对密品进行参观。

密品研制、生产过程中涉及国家秘密的零件、部件、组件等物品,也应当指定专人保管并履行登记手续。研制、生产过程中包含密品涉密信息的文件、资料、图纸、图表及其他资料,应当按照涉密载体进行管理。

(三)密品的运输与移交

密品的运输与移交环节应当按规定履行审批、交接、签收手续,并保存记录备查。

运输前应当将密品密封于包装箱内,无法置于包装箱内的,应当采取其他安全保密措施。小件密品需要邮寄的,应当通过机要交通或者机要通信邮寄。需要随身携带的,必须两人以上同行,采取严密的保护措施。

密品运输应当确定运输安全负责人,对押运人员进行保密教育,制定安全保密方案,经单位领导审批后落实,选择安全的路线、时间,采取安全可靠的押运措施,两人以上押运,必要时武装押运,并尽可能依照国家有关规定办理免检手续。

密品运输过程中不得随意改变确定的行车路线,不得随意停车,严禁无关人员搭乘。需要停靠时,车上应当留人负责密品的安全。

(四)密品的保存与使用

密品应当存放在具备安全保密防范措施的场所,实行集中、专人管理,并完善管理制度,严格控制人员进出。体积较大、不能及时存放在安全保密场所的,应当采取保护性措施。

密品带出保存场所使用,应当做好使用记录,使用后及时归还。因工作需要到校外使用密品时,应当按规定履行审批手续,外出过程中应当保证密品的安全。

通过特殊渠道获取的密品,应当采取相应的保密措施,不得因使用而

使无关人员知悉密品来源和保密内容。

密品保存使用过程中应当严格控制接触范围，未经批准严禁无关人员参观密品或拍照录像等，经批准后应当使用涉密设备进行拍摄。

（五）密品的维修与销毁

密品需要维修时，应当履行审批手续，审批通过后方可进行维修。

密品的检修和维修工作一般不得由境外人员承担，确需境外人员承担时，应当依照规定履行审批手续并采取相应的保密措施。

密品由外来人员进行现场维修时，应当由专人全程监督，禁止维修人员擅自恢复、读取和复制密品中含有的涉密信息。需要带离保存现场进行维修的，应当按保密管理有关规定送到指定维修地点，并与维修单位签订保密协议。

密品销毁时应当履行审批手续，在销毁密品过程中应当符合以下要求：

（1）选择有保密保障条件的部门、单位或场所进行；

（2）指定专人监销；

（3）确保密品被销毁后不再具有国家秘密信息；

（4）外形上能直接反映国家秘密的密品，应当彻底毁形；

（5）对仍有保密价值的碎屑、粉末、液体等残留物质，应当及时收集并妥善处理。

高校应当建立完善的涉密载体和密品的保密管理制度，切实加强涉密载体和密品保密管理，健全监督检查机制，把涉密载体和密品管理情况作为保密监督检查的重要内容。

附表 6-1　涉密载体制作审批表示例

涉密载体制作审批表

<table>
<tr><td colspan="2">院系（部、处）</td><td colspan="2"></td><td colspan="2">申请人</td><td></td></tr>
<tr><td colspan="2">制作原因</td><td colspan="2"></td><td colspan="2">载体去向</td><td></td></tr>
<tr><td colspan="2">制作地点</td><td colspan="3">□本单位</td><td colspan="2">□校定点复印室</td></tr>
<tr><td colspan="2">载体来源介质</td><td colspan="5">□涉密输出专用 U 盘　　编号：________
□纸介质　　编号：________</td></tr>
<tr><td rowspan="6">载体明细</td><td>制作方式</td><td>载体编号</td><td>文件名称</td><td>密级</td><td>份数</td><td>页数/每份</td></tr>
<tr><td>□打印</td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>□复印</td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td rowspan="3">□刻录</td><td>光盘编号</td><td colspan="2">包含文件名称</td><td colspan="2">密级</td></tr>
<tr><td></td><td colspan="2"></td><td colspan="2"></td></tr>
<tr><td></td><td colspan="2"></td><td colspan="2"></td></tr>
<tr><td colspan="2">项目负责人意见</td><td colspan="5">同意（　）　　不同意（　）
签字：
年　月　日</td></tr>
<tr><td colspan="2">单位保密负责人意见</td><td colspan="5">同意（　）　　不同意（　）
签字：（盖章）
年　月　日</td></tr>
<tr><td colspan="2">登记签收</td><td colspan="2">以上操作已完成。
操作人签字：
年　月　日</td><td colspan="3">以上载体已领取。
领取人签字：
年　月　日</td></tr>
</table>

附表 6-2　涉密载体制作收发受控登记表（管理员）示例

涉密载体制作收发受控登记表（管理员）

序号	日期	类型	来源	名称或内容	密级	数量	页数/份 文件数/张	受控编号	去向	领用 签字

附表 6-3　涉密载体台账登记示例

涉密载体台账

序号	登记日期	类型	来源	名称或内容	编号	密级	数量	页数	责任人	备注

附表 6-4　涉密载体收发登记本（个人）示例

涉密载体收发登记本（个人）

序号	日期	类型	来源	名称或内容	密级	数量	页数/份 文件数/张	受控编号	去向	

附表 6-5　涉密载体处理记录单（管理部门）示例

涉密载体处理记录单（管理部门）

来源单位		处理事由	
载体类型		密级	
载体编号		经办人	
名称或内容			
处理意见	□复制转发　□组织阅读　□原文传递　□其他____ ____ 知悉范围：____________________ 审批人（签字）：　　　年　月　日		

阅读、复制—转发载体信息登记

日期	阅读/复制—转发 纸件（编号/页码/页数/密级） 光盘（编号/内容/密级）	单位	签字	备注

附表 6-6　机要文件收发登记表示例

机要文件收发登记表

序号	来文单位	机要号	机要密级	收件人	收件单位	文件名称	发文字号	密级	份数	页数	接收时间	签收人	备注

附表 6-7　机要文件发送记录单示例

机要文件发送记录单

<table>
<tr><td>申请人</td><td colspan="2"></td><td>所在单位</td><td colspan="4"></td></tr>
<tr><td>联系电话</td><td colspan="7"></td></tr>
<tr><td>机要文件类型</td><td colspan="7">☐文件　☐学生档案　☐人事档案　☐项目材料　☐其他________
__________</td></tr>
<tr><td>发送机要事由</td><td colspan="7"></td></tr>
<tr><td>机要接收单位</td><td colspan="7"></td></tr>
<tr><td colspan="3">文件标题(或名称)</td><td colspan="2">密级</td><td>份数</td><td>每份页数</td><td>编号</td></tr>
<tr><td colspan="3"></td><td colspan="2"></td><td></td><td></td><td></td></tr>
<tr><td>项目负责人意见</td><td colspan="7">(非科研项目无须填写此栏)
项目负责人签字：
年　月　日</td></tr>
<tr><td>所在单位意见</td><td colspan="7">已确认上述机要文件登记信息与信封内文件资料相符,其中涉密文件已按照学校涉密载体管理规定履行制作审批手续。
机要文件主管领导签字：
(公章)
年　月　日</td></tr>
<tr><td>机要收发室登记</td><td colspan="7">经办人签字：
年　月　日</td></tr>
</table>

附表 6-8　涉密载体校外处理审批记录单示例

涉密载体校外处理审批记录单

<table>
<tr><td colspan="2">申请人</td><td colspan="2"></td><td>单位</td><td colspan="3"></td></tr>
<tr><td colspan="2">携带载体
人员涉密等级</td><td colspan="6">☐核心　　☐重要　　☐一般</td></tr>
<tr><td colspan="2">校外处理单位</td><td colspan="6"></td></tr>
<tr><td colspan="2">事由</td><td colspan="6">☐汇报交流　　☐载体上交　　☐其他______</td></tr>
<tr><td colspan="2">项目负责人意见</td><td colspan="6">负责人（签字）：　　年　　月　　日</td></tr>
<tr><td colspan="2">所在单位意见</td><td colspan="6">保密负责人（签字）：　　年　　月　　日</td></tr>
<tr><td rowspan="4">携带载体信息</td><td>类型</td><td>光盘编号</td><td>包含文件的名称</td><td colspan="2">密级</td><td>处理方式</td><td>接收人
签字</td></tr>
<tr><td>☐光盘</td><td></td><td></td><td colspan="2"></td><td></td><td></td></tr>
<tr><td rowspan="2">☐纸介质</td><td>载体编号</td><td>文件或资料名称</td><td>密级</td><td>页数/份</td><td>处理方式</td><td>接收人
签字</td></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td colspan="2">备注
（资料带回情况）</td><td colspan="6">经办人签字：</td></tr>
</table>

附表 6-9　借阅涉密载体审批登记表示例

借阅涉密载体审批登记表

序号	名称或内容	编号	密级	份数	页数	审批人	借用目的	借用人	借用时间	归还时间	经办人	备注

附表 6-10　涉密档案利用申请表示例

涉密档案利用申请表

申请人		所在单位	
利用档案类别	□科研项目　□学位论文　□博士后报告　□文书档案		
文件名称及受控编号 （可附件）		密级	
利用类别	□阅览　□外借　□复印（涉密载体请另填写制作审批表） □其他		
利用内容及原因			
经办人姓名		证件号	
档案负责人意见	利用内容包含敏感信息：□是　□否 □同意阅览 □同意复印/外借 签字： 年　月　日		
归档单位 保密负责人意见	签字：（公章） 年　月　日		

附表 6-11　销毁涉密载体审批表(纸介质)示例

销毁涉密载体审批表(纸介质)

审批单号:

<table>
<tr><th>序号</th><th>申请人</th><th>内容或名称</th><th>编号</th><th>密级</th><th>份数(数量)</th><th>页数/份</th><th>责任人签字</th></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>院系审批意见</td><td colspan="7">同意(　)　　　不同意(　)
保密负责人签字:　　　　　　年　　月　　日</td></tr>
<tr><td>院系监销经办</td><td colspan="7">以上拟销毁载体清点核对无误并封装。
监销经办签字(2 人):　　　　　　年　　月　　日</td></tr>
<tr><td>学校复核接收意见</td><td colspan="7">同意接收。
保密办经办人签字:　　　　　　保卫部经办人签字:
年　月　日　　　　　　年　月　日</td></tr>
</table>

附表 6-12　涉密载体销毁记录单示例

涉密载体销毁记录单

<table>
<tr><td rowspan="3">销毁单号</td><td>销毁单编号</td><td>销毁单编号</td><td>销毁单编号</td><td>销毁单编号</td><td>销毁单编号</td></tr>
<tr><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td rowspan="2">销毁地点</td><td colspan="2" rowspan="2"></td><td rowspan="2">销毁方式</td><td colspan="2">纸介质:焚烧(　)　粉碎(　)</td></tr>
<tr><td colspan="2">磁介质:　物理销毁(　)</td></tr>
<tr><td>销毁时间</td><td colspan="2"></td><td>监销人
(2 人)</td><td colspan="2"></td></tr>
</table>

第七章　科研场所保密管理

科研场所是科研活动发生和科研成果产生和保存的主要场所，也是科研设备和载体存放的集中场所。对于涉密科研项目来说，科研场所是非常重要的保密管理要素。

为了做好科研场所的保密工作，首先需要清晰界定开展涉密科研生产活动或保管、存放涉密载体、涉密设备的场所，即明确哪些场所涉密，并根据涉密事项多少、涉密程度深浅进行分级分类管理；其次，为了降低管理成本和减少失泄密风险，保证管理效果，涉密设备、涉密载体存放场所与涉密科研活动场所应当尽可能实现集中管理；同时，应当将涉密课题组开展非涉密科研活动的场所也纳入保密管理范围。

一、保密要害部门、部位管理

保密要害部门、部位是涉密科研场所保密管理的重中之重。保密要害部门、部位的管理主要包括准确界定（包含确定、变更和撤销）、防护措施建设（含人防、技防与物防）以及日常运行管理三部分内容。

（一）职责与分工

一般来说，学校保密委员会负责校级保密要害部门、部位的审批工作；保卫处负责审定学校各保密要害部门、部位的防护建设方案，并对安全保密防范设施进行验收；保密管理办公室负责对学校保密要害部门、部位的

保密管理工作进行指导、监督和检查;学校所属各单位依据“谁主管、谁负责”的原则,负责本单位保密要害部门、部位的日常管理工作。

(二)保密要害部门、部位的确定

保密要害部门、部位确定的一般原则、标准及程序如下。

1. 保密要害部门、部位的确定原则

(1)最小化原则:坚持将学校最小的行政单位确定为保密要害部门,比如,可以将科室确定为保密要害部门的,不定到部处,能定到所/中心的,不定到院系;

(2)最少化原则:在保证涉密科研生产活动正常开展的情况下,将学校所属各单位产生、处理、保管国家秘密的涉密场所按区域或院系尽可能集中在同一楼宇、同一楼层、同一区域或房间中;

(3)保密要害部门内部一般包括一个或若干个保密要害部位,保密要害部门内部可以进一步确定保密要害部位。

2. 保密要害部门、部位的确定标准

(1)将学校科研、管理等工作中产生、传递、使用和管理绝密级或较多机密级、秘密级国家秘密事项并列入学校编制的机构,确定为保密要害部门,如机要科、军工科研管理部门;

(2)将学校各单位内部集中制作、存储、保管绝密级国家秘密载体或较多机密级、秘密级科研项目文件、资料、成果等国家秘密载体的专用、独立、固定场所,以及承担绝密级或较多机密级,以及大量秘密级武器装备相关项目的研制、生产、试验场所,确定为保密要害部位,如涉密档案室、涉密机房、涉密实验室、密品库房等。

根据产生或保管的国家秘密事项情况,保密要害部位可以进一步划分为三个等级。

(1)将产生或保管的国家秘密事项对国家安全和国防科技工业全局具有重大影响,一旦泄密或被窃密,会给国家安全和利益造成特别严重损害的部位界定为一级保密要害部位,如重点型号总体设计室、科技档案室。

（2）将产生或保管的国家秘密事项对本行业、本系统和本单位具有重要影响，一旦泄密或被窃密，将给国家安全和利益造成重大损害的部位界定为二级保密要害部位，如重点型号分系统设计室、科技档案室。

（3）将其他以产生或保管军品预研及配套任务国家秘密事项为主的保密要害部位，一旦泄密或被窃密将给国家安全和利益带来一定损害的部位界定为三级保密要害部位，如以秘密级事项为主的保密室或资料室。

3. 保密要害部门、部位的确定/调整程序

（1）学校所属各单位，应当依据保密要害部门、部位的确定原则，会商学校保密管理办公室与业务主管部门，对本单位达到保密要害部门、部位确定标准的机构或场所，提出确定申请（参见附表7-1），并组织开展安全防护措施与保密管理制度建设，经学校保密、保卫部门现场检查验收合格后，报学校保密委员会审批。确定流程参见图7-1。

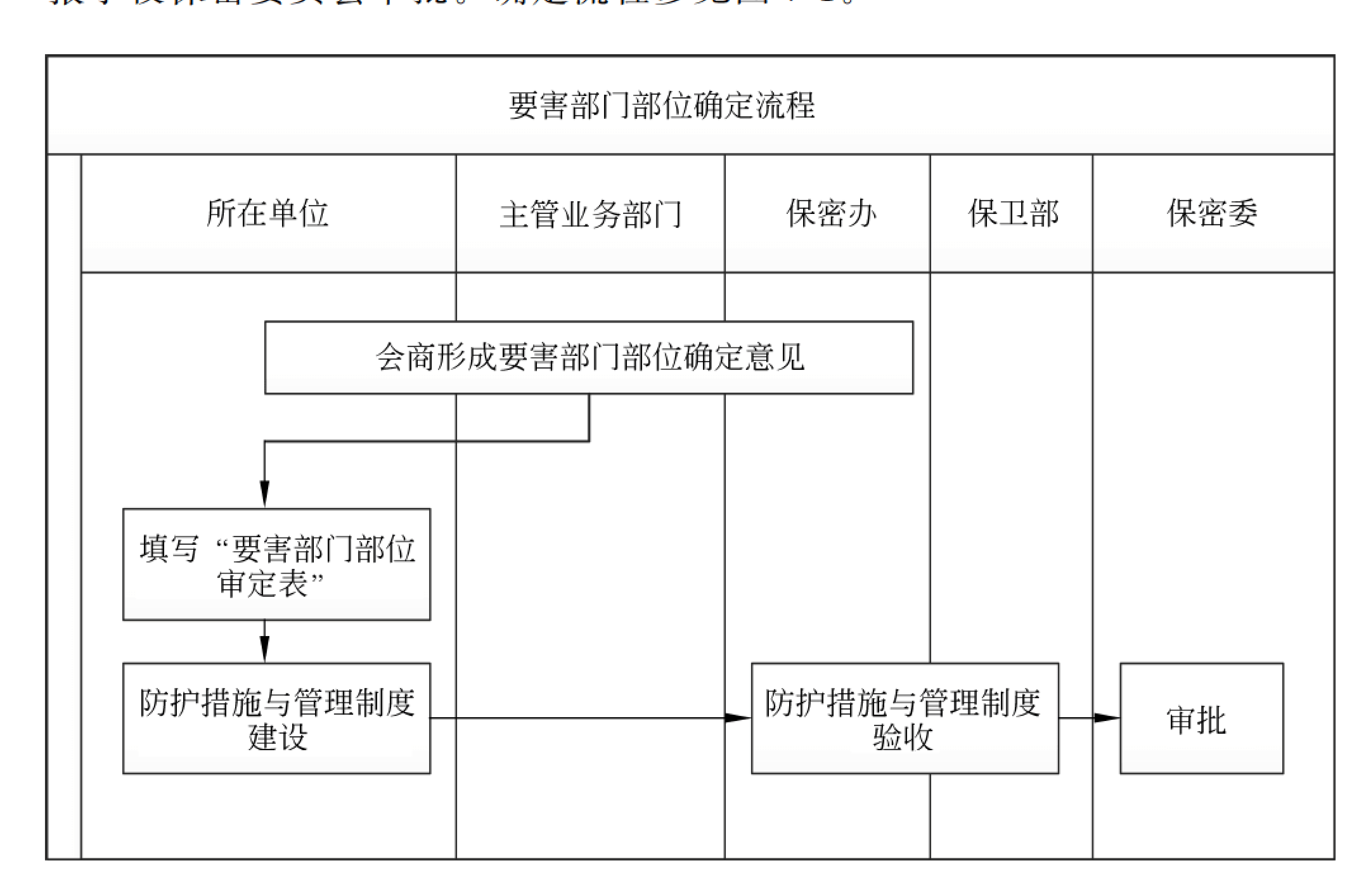


图7-1　要害部门部位确定流程

（2）各单位应当根据情况变化，适时对保密要害部门、部位做出相应调整，提出变更或撤销申请，履行与确定保密要害部门部位相同的审批程序，

并根据变更或撤销后场所的防护等级落实安全防护措施与保密管理要求。

学校保密管理办公室每年度对全校保密要害部门、部位进行一次审核，并按要求及时将新增及变更、撤销情况报当地国家保密行政管理备案。

（三）保密要害部门、部位的安全防护措施

为了加强保密要害部门、部位的安全防范，其所属二级单位应当按照有关保密法律、法规和标准规定要求，结合本单位保密要害部门、部位的实际情况，进行安全防护措施设计和建设，按标准建设或配备技术防护措施、物理防护措施与人防措施（简称技防、物防与人防）。技防措施主要包括视频监视系统、门禁系统、红外/微波对射防盗报警装置以及碎纸机、光盘粉碎机、手机屏蔽柜等；物防措施是指“三铁一器”，即铁门、铁窗、铁柜（密码文件柜或密码保险柜）与防盗报警器；人防措施一般包括武警值勤、保安执勤和内部职工值班。

1. 建设标准

（1）保密要害部门应当实行区域隔离，保密要害部位应当实施物理防护。出入口须安装视频监控装置、防盗铁门，视频监控记录保存时间不少于三个月；门禁系统要采取IC卡与密码并用或生理特征（如虹膜、指纹）进行身份鉴别，窗户须安装防盗铁窗或在其周边安装红外/微波对射防盗报警装置。安防监控室配备值班人员，保密要害部门、部位比较集中的区域或涉及绝密级国家秘密的保密要害部位应当根据需要配备值班或警卫人员。

（2）内部须安装防盗报警装置，配备密码文件柜、碎纸机、光盘粉碎机、手机屏蔽柜等设备，存储绝密级国家秘密的还需配备密码保险柜。

（3）校内有举办涉密会议需求的，配备手机干扰仪或会议保密机等设备。

（4）校内有绝密级机房以及召开绝密级会议需要的，考虑按标准建设屏蔽机房及保密会议室。

2. 建设程序

（1）由保密要害部门、部位所属二级单位提出建设需求，根据学校保密管理办公室提供的具备涉密安防监控资质的建设施工单位名录中选择建

设施工单位。

（2）由建设施工单位提出保密要害部门、部位的安全保密防范建设方案，并报保卫处、保密管理办公室审核。

（3）由建设施工单位按审核通过的方案施工。

（4）由保卫部组织对施工及相关防护设备进行技术验收。

（5）由保密要害部门、部位所属单位购置符合国家技术标准的必需的安全防护设备，如手机屏蔽柜、密码文件柜等。

（6）由保密管理办公室进行安防措施、管理措施综合审核，通过后方能使用。建设程序参见图 7-2。

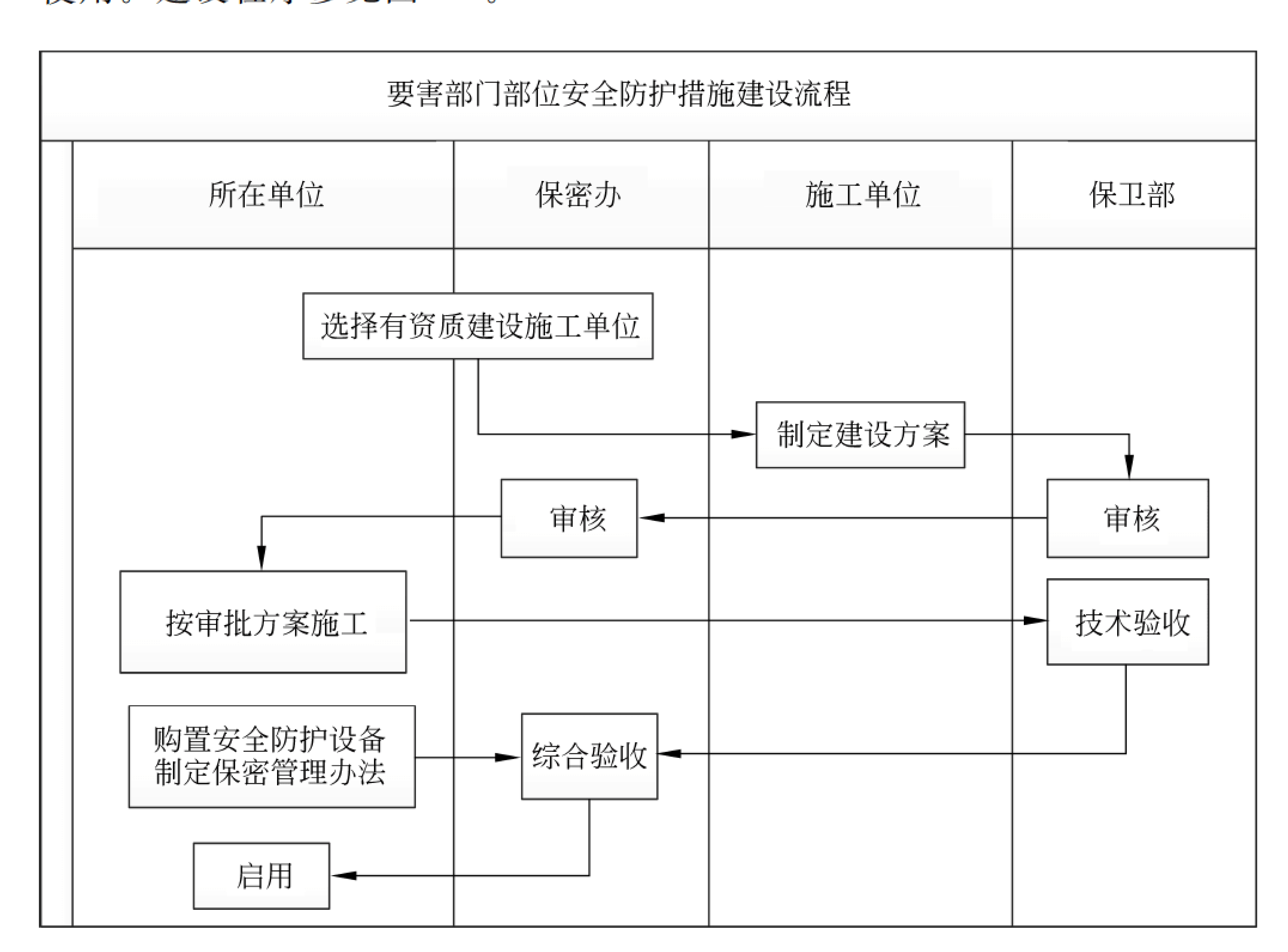


图 7-2　要害部门部位安全防护措施建设流程

保密要害部门、部位在建、改建、扩建工程中，要与保密防护措施同计划、同预算、同建设、同验收。

（四）保密要害部门、部位的日常管理

为了确保国家秘密安全，保密要害部门、部位除了要求技防、物防、人防措施到位，还要建立完善的保密保卫管理制度，一般包括：

1. 进出管理

（1）建立保密要害部门、部位红名单、白名单与黑名单。红名单是指因研究或管理工作需要在此要害部门、部位开展涉密工作的人员名单，一般包括要害部门、部位所属单位内部的涉密人员，以及需要经常进出该部门部位的明确允许进入的人员，在摄像、门禁等可追溯进出情况，可授权红名单内人员免登记；白名单是指确因工作需要进入保密要害部门、部位的非授权人员，需经本部门、部位负责人批准，并做好登记工作，在保密要害部门、部位内部工作人员的陪同和监督下开展相关活动；黑名单是指与本部门工作无关的人员（含快递人员），包括外国人（含港澳台人员），应当严禁其进入，有条件的，保密要害部门内设置接待室，与涉密区域隔离分开。

（2）出入口应当配备手机屏蔽柜。

（3）按要求配备值班人员的保密要害部门部位还应当填写值班记录表。

2. 内部管理

（1）内部禁止安装、使用无绳电话、无线鼠标等具有无线通信功能的设备。

（2）未经批准，不得将具有无线通信功能的设备和具备拍摄、录音等功能的电子设备带入保密要害部门、部位。

（3）严禁将手机带入保密要害部门、部位。

（4）每天首先到岗及最后离岗的人员应当对保密要害部门、部位的状态进行检查确认，发现异常及时处理。

（5）对保密要害部门、部位的安全防护设施运行情况进行经常性的检查，确保技防和物防设施正常工作。

（6）对内部人员开展经常性的保密宣传教育，努力提高内部人员的保

密意识和技能。

（7）对内部安全保密制度落实情况定期进行检查，填写记录表，及时发现和消除安全隐患。

（8）保密要害部门、部位内、外部情况发现变化时，应当及时向学校保密管理办公室报告，并采取针对性措施。

3. 参观、接待管理

（1）保密要害部门、部位接待参观、接待，必须事先履行审批手续（参见附表 7-2）。

（2）接待、参观人员进入保密要害部门、部位前，需明确保密管理要求，禁止携带手机、相机、录音笔等有录音、录像、拍照等功能的设备进入。

4. 工勤服务人员管理

（1）保密要害部门、部位的工勤服务人员在其进入工作岗位前，由其聘用单位委托有关单位对其进行政治审核，确认合格，接受保密培训并在其签订保密承诺书后，方可进入工作岗位。

（2）工作期间，须明确专人管理，在划定区域内活动，禁止单独进入保密要害部位。

5. 监控室管理

（1）应当配备值班人员，对值班人员上岗前审查可参照工勤服务人员管理。

（2）应当明确监控室值班人员岗位职责，双人双岗，24 小时对保密要害部门、部位进出进行监控，发现异常马上向保密要害部门、部位联系人报告。

（3）应建立应急预案，监控室值班人员应当技术熟练、训练有训，能够及时有效处理紧急情况。

（4）保密要害部门、部位负责人至少每个月组织对视频监控内容进行回看，及时处理发现和反映的问题。

除了遵守以上通用管理要求外，各保密要害部门部位可以结合实际情况，制定有针对性和操作性的管理办法，并张贴在涉密区域，如涉密资料

室/涉密档案室应当对允许进出人员、资料/档案的利用(包括提供、阅览、借阅、复制、保存等)等作出具体规定。

二、其他涉密场所的保密管理

对于保存、处理涉密信息但涉密等级及数量达不到保密要害部门、部位标准的学校其他涉密场所,如涉密资料室、涉密机房、涉密办公室、涉密实验室以及涉密会议室和涉密外场试验场地等一些临时的涉密场所,应当根据规定,分别提出相应的防范措施与保密管理要求。

(一)涉密会议室

学校主办或承办涉密会议的单位,应当选择具备安全保密条件的场所作为涉密会议室,一般尽可能选择军方指定场所或单位内部会议室,严禁选择涉外宾馆、饭店、招待所以及外资、中外合资单位的会场。会前,应当明确专人负责安全保密工作,根据涉密会议密级和工作需要,确定参会人员范围,制定保密工作方案并报批(参见附表 7-3)。密级高或参会人员多的重要涉密会议(会议内容或者发放的载体涉及机密级(含)以上国家秘密,且参会人数达到 50 人以上或者参会人数达到 100 人以上的秘密级会议),主办或承办单位应当制定专门的保密工作预案,指定专人落实保密措施,必要时学校保密管理办公室应当派人进行监督和检查(参见附表 7-4)。

涉密会议的保密管理一般包括会前、会中、会后三个阶段。

1. 会前准备及安全保密检查

(1)须在会场入口的显著位置摆放保密提醒标志,禁止带入具有无线联网功能的计算机和智能终端(含笔记本电脑、平板电脑、手机等)等设备,并配备手机柜。

(2)会场内不得使用无线话筒、对讲机等无线扩音设备,关闭会场所有不使用的视频会议设备,并放置无线干扰设备。

(3)会议使用的计算机、投影仪、录音等设备应当符合保密要求。

（4）对服务人员进行身份确认，必要时自行安排服务人员。

（5）对会议工作人员和服务人员进行保密教育，明确保密纪律和要求。

2. 会议期间保密措施

（1）对进入会场的人员核对身份，确保参会人员身份准确无误，并履行签到手续；

（2）提醒与会者存放手机，不得将具有无线联网功能的便携设备带入会场；

（3）除了会议安排的拍摄、录音设备，不得将其他具有拍摄、录音功能的设备带入会场；

（4）发放涉密资料，须履行编号登记手续；

（5）会前应当向与会人员进行保密提醒；

（6）会议期间，指派专人管理文件资料，提醒与监督与会者不得擅自带出会议场所，休会时会议资料集中管理，会议结束后要履行清退登记手续；

（7）会议如需记录应当按照涉密载体进行管理；

（8）经批准制作的会议声像资料等同密级文件进行管理；

（9）安排专人负责会议期间会场外区域的安全保密管控，禁止无关人员进入。

3. 会后安全保密检查

（1）清点会议资料与设备；

（2）对会场、客房、餐厅等地进行安全检查，防止涉密载体等文件、设备丢失；

（3）将带回的涉密文件、资料做好登记和管理，并根据需要及时销毁。

（二）涉密外场试验

为了检验武器装备设计方案和战术指标性能的有效性或产品质量的可靠性，承担任务总体或重要分系统的校内承研单位，根据需要可能要在校外一定的空域、地域、水域进行一系列试验验证活动，即外场试验。试验

现场的保密管理工作由外场试验牵头单位负责组织协调，应当根据试验内容、试验场所周围环境、参加试验单位和人员情况，制定或提出具体的保密防范措施与工作要求，参加单位应当接受牵头单位和试验厂区所在单位的保密管理。

学校参加外场试验的承研单位应当指定一名负责人，负责外场试验的保密管理工作，并制定专项保密工作方案，报学校保密管理办公室审批（参见附表 7-5）。保密方案应当结合具体试验任务情况制定，除了明确任务性质、项目或型号密级、组织领导之外，重点对参试人员、密品密件运输与管理、数据交换与现场通信等明确保密管理措施，提出具体要求等，试验期间定期向学校保密管理办公室报告保密管理情况并接受监督检查。主要包括：

1. 外场试验前参试人员资格审查及行前保密教育

（1）对参试人员进行资格审查，并组织签署保密承诺书；

（2）对参试人员开展保密宣传教育。

2. 密品运输保密管理

（1）学校参加外场试验的承研单位须提前办理免检申请，由学校保密、保卫主管部门协助办理免检证明。

（2）乘坐公共交通工具运输时，应当密封包装，做到件不离人，必要时 2 人同行。

（3）专车运输时，应当提前制定运输方案，经保卫、保密主管部门审批后方可实施（参见附件 7-6），包括：对密品进行密封或遮盖处理；安排 2 人以上随行人员，严禁无关人员搭乘；提前确定行车路线、中途停靠点以及安全警卫措施；不得向无关人员泄漏运行时间、路线等情况；已确定的行车路线未经学校保卫、保密主管部门批准不得改变，不得随意停车，停车期间专人值守。

3. 试验现场保密管理

（1）外场试验单位保密负责人要指定专人负责本单位在试验现场的设备及文件资料管理工作；

（2）大型或密级较高的试验现场，严格实行出入证制度，出入证的发放、保管要有完备的登记手续和管理制度；

（3）应当妥善保管参试单位试验记录、设备器材，牵头单位和试验厂区所在单位应当为涉密载体保存、制作、传递等提供符合保密要求的设备与渠道；

（4）加强现场参试人员的住宿管理，平时在住处应当安排人员留守值班，值班人员要时刻提高警惕，确保住处存放的国家秘密载体安全；

（5）加强现场通信管理，参试人员联系工作、汇报情况时，禁止用普通电话、电报、传真等传递涉密信息。大型或密级较高的试验现场禁止参试人员携带手机；

（6）未经批准试验现场不得录像、摄像，妥善保管经批准拍摄的录像带（包括原始素材）、照片（包括底片），不得随意复制和向外提供；

（7）未经批准不得组织现场参观活动。经批准的参观活动必须按照指定路线与保密方案进行，介绍情况要适度，并对参观的基本情况做出文字记载。

4. 试验后保密检查与总结

（1）清点密品、涉密资料、试验设备与试验记录；

（2）对试验现场、宿舍等地进行安全检查，防止涉密载体、设备等遗落；

（3）对带回的涉密文件、资料做好登记和管理；

（4）将试验保密管理工作作为试验工作总结的必备内容之一，与试验工作总结一同存档。

（三）专用涉密资料室/涉密机房

尽管专用涉密资料室或涉密机房保存、处理的涉密信息的涉密等级或数量不及保密要害部位，作为集中存放或处理涉密信息的涉密场所，其所属二级单位仍然应当参照保密要害部位管理要求对其进行安全防范措施建设与日常管理。包括安装视频监视系统和/或门禁系统、“三铁一器”，配备碎纸机、光盘粉碎机等，对涉密资料室/涉密机房进出、涉密资料及涉密

设备的管理与利用等作出明确规定，并在涉密场所内张贴。

（四）涉密办公室/实验室

一些项目负责人承接有关涉密项目，但单位暂时不具备涉密场所的集中条件，只能对其现有办公室或实验室进行改造，开辟出空间独立的涉密区域，配备防盗门、防盗窗、保密柜等基本防护设施，禁止无关人员进入。

对于存放涉密实验设备的实验室，除了安装防盗门、防盗窗等基本防护措施外，还应当制定并张贴有关管理办法，对涉密实验室的进出、涉密实验设备日常防护及实验时的保护、实验室内部管理（如禁止拍照等）作出明确规定。

（五）涉密课题组非涉密场所

由于涉密课题组接触和处理涉密信息，其课题组成员工作的非涉密场所的保密管理也应当纳入保密管理范围，主要做到：加强保密教育提醒，包括张贴保密提醒标语，与课题组成员签订保密协议，利用学术讨论会等各种机会强调保密纪律等；加强保密管理，不允许将个人计算机、移动存储介质等设备带入工作场所，不允许私自将同学、同事、朋友等外来人员带入工作场所；加强保密检查，重点是载体和计算机检查，确保不在非涉密场所存放涉密载体，不使用非涉密计算机处理涉密信息。

附表 7-1　保密要害部门、部位审定表示例

保密要害部门、部位审定表

<table>
<tr><td colspan="2">部门(位)名称</td><td colspan="2"></td><td>类别</td><td>□ 部门　□ 部位</td></tr>
<tr><td colspan="2">负责人</td><td colspan="2"></td><td>联系电话</td><td></td></tr>
<tr><td colspan="2">涉密等级</td><td colspan="2"></td><td>涉密人员数</td><td></td></tr>
<tr><td colspan="2">地点</td><td colspan="4"></td></tr>
<tr><td colspan="2">申报理由</td><td colspan="4"></td></tr>
<tr><td colspan="2">保密制度</td><td colspan="4">(附管理办法)</td></tr>
<tr><td colspan="2">防护情况</td><td colspan="4">人防
技防
物防</td></tr>
<tr><td>单位保密负责人意见</td><td>签字(公章)：
年　月　日</td><td>保卫部意见</td><td>(安全防护措施方面)
负责人签字(公章)：
年　月　日</td><td>保密办综合审核意见</td><td>负责人签字(公章)：
年　月　日</td></tr>
<tr><td colspan="2">保密委审批意见</td><td colspan="4">负责人签字(公章)：
年　月　日</td></tr>
</table>

附表 7-2　涉密场所接待参观保密审查表示例

涉密场所接待参观保密审查表

涉密场所地点	
涉密事项密级	密级：秘密（　）、机密（　）
来访单位及人数	
接待人	
接待安排	（明确是否允许拍照、录音、录像）
参观路线	
课题负责人意见	签字：　　年　月　日
系保密工作负责人意见	签字：　　年　月　日
业务主管部门意见	签字：　　年　月　日
校保密办审定意见	签字：　　年　月　日 （盖章）

附表 7-3　涉密会议保密审批表示例

涉密会议保密审批表

<table>
<tr><td>会议名称</td><td></td><td>主办单位</td><td></td></tr>
<tr><td>承办单位</td><td></td><td>密级</td><td></td></tr>
<tr><td>会议时间</td><td></td><td>会议地点</td><td></td></tr>
<tr><td>会议保密负责人</td><td></td><td>联系方式</td><td></td></tr>
<tr><td>参加会议
单位及人员</td><td colspan="3">（可附页）</td></tr>
<tr><td>保密工作方案</td><td colspan="3">1. 人员管理
明确工作人员范围和参加人员范围，履行签到手续（　）
对参会人员进行资格审查和保密提醒（　）
2. 载体管理
• 不发放涉密载体（　）/ 指派专人管理涉密载体，履行编号登记发放手续，会议结束后履行清退、销毁工作（　）
• 与会人员不允许记录（　）/ 记录资料按涉密载体管理（　）
3. 设备管理
• 禁止将手机和其他具有无线上网功能的设备带入会场（　）
• 配备手机信号干扰仪（重要会议必须配备）（　）
• 不使用无线话筒、对讲机等无线扩音设备（　）
4. 录音、照相、摄像
• 不录音（　）、照相（　）、摄像（　）/
• 指定专人使用涉密设备录音（　）、照相（　）、摄像（　），并按涉密载体管理（　）
5. 会后检查
• 对会场、客房、餐厅等地进行安全检查（　）
6. 其他
会议保密负责人签字：　　　　年　　月　　日</td></tr>
<tr><td>会议主办单位意见</td><td colspan="3">☐ 同意保密工作方案 ☐ 不同意保密工作方案
其他：
主办单位领导签字：　　　　年　　月　　日</td></tr>
<tr><td colspan="2">院（系、所）保密领导小组意见
☐ 同意保密工作方案
☐ 同意举办涉密会议
其他：
负责人签字（盖章）：
年　　月　　日</td><td colspan="2">保密办意见（对重要涉密会议）
☐ 同意保密工作方案
☐ 同意举办涉密会议
其他：
负责人签字（盖章）：
年　　月　　日</td></tr>
</table>

附表 7-4　涉密会议保密审查表示例

涉密会议保密检查表

承办单位		主办单位	
会议保密负责人		联系电话	
检查方式	□主办/承办单位监督检查　□保密办监督检查		
项　目	检 查 内 容		
会议类别	□ 一般涉密会议 □ 重要涉密会议		
组织结构及职责	1. 主办单位是否对会议安排进行指导和监督　□是　□否 2. 承办单位是否清楚涉密会议相关要求　□是　□否 3. 是否制定了会议的安全保密方案　□是　□否		
涉密会议保密管理情况	4. 是否确定工作人员范围和参加人员范围　□是　□否 5. 是否对人员进行保密教育和审查　□是　□否 6. 是否履行涉密会议签到手续　□是　□否 7. 涉密载体是否由专人管理　□是　□否 8. 涉密载体是否履行编号登记发放手续　□是　□否 9. 会议结束后是否认真履行清点、登记、销毁工作　□是　□否 10. 是否按要求记录涉密事项　□是　□否 11. 是否按会议保密方案进行录音、照相、摄像　□是　□否 12. 是否未使用无线话筒、对讲机等扩音设备　□是　□否 13. 会场是否开启手机信号干扰仪　□是　□否 14. 手机等具有无线上网功能的设备是否带入会场　□是　□否 15. 会议结束后，会务人员是否对会议使用的会场、客房、餐厅等地进行安全检查，防止会议文件等遗落丢失　□是　□否		
负责人签字	会议保密负责人签字： 年　月　日		
	保密办监察人签字（保密办监督检查时需此项）： 年　月　日		

附表 7-5　外场试验保密审批表示例

外场试验保密审批表

<table>
<tr><td>申请单位</td><td></td><td>外场试验牵头单位</td><td></td></tr>
<tr><td>试验时间</td><td></td><td>试验地点</td><td></td></tr>
<tr><td>任务密级</td><td></td><td>试验现场保密负责人</td><td></td></tr>
<tr><td>参加试验人员</td><td colspan="3">附《参加外场试验人员信息登记表》</td></tr>
<tr><td>主要试验内容</td><td colspan="3">保密负责人(签名)：　　年　月　日</td></tr>
<tr><td>保密方案</td><td colspan="3">1. 参试人员管理
• 参试前,对参加试验人员进行保密教育,提出保密要求　(　)
• 参试人员与负责人签署保密责任书　(　)
2. 密品密件运输
• 提前办理免检证明　(　)
• 乘坐公共交通工具运输,密封包装,件不离人　(　)
• 专车运输时,提前制定运输方案　(　)
3. 试验现场管理
• 制定试验场区保密管理规定(对牵头单位)　(　)
• 严格遵守牵头单位制定的试验场区保密管理规定　(　)
• 定期对试验现场的保密管理情况进行检查　(　)
4. 数据交换与现场通信管理
• 严格控制具有摄录功能的设备带入涉密试验现场　(　)
• 不通过无保密保障措施的手机等通信设备谈论试验情况　(　)
• 使用符合保密要求的设备保存试验结果　(　)</td></tr>
<tr><td colspan="2">院(系、所)保密领导小组审核意见

负责人签字(盖章)：
年　月　日</td><td colspan="2">业务主管部门审查意见

负责人签字(盖章)：
年　月　日</td></tr>
<tr><td>保密办审批意见</td><td colspan="3">审定人签章：
(盖章)　　年　月　日</td></tr>
</table>

附表 7-6　密品押运保密审批表示例

密品押运保密审批表

编号：　　　　　　　　　　　　　　填报日期：　年　月　日

单　位			
产品名称		涉密等级	
运输路线			
运输工具			
保密措施	1. 对密品进行密封（　）/遮盖处理（　）； 2. 安排 2 人以上随行人员； 3. 行车路线； 4. 中途停靠点； 5. 停靠期间安全警卫措施； 6. 严禁无关人员搭乘，不得向无关人员泄露运行时间、路线等情况； 7. 其他。		
院（系、所）保密领导小组审核意见	负责人签字（盖章）： 年　月　日		
保卫部审核意见	负责人签字（盖章）： 年　月　日		
保密办审批意见	负责人签名（盖章）： 年　月　日		
保密/保卫部门跟踪检查情况	检查人： 年　月　日		

第八章　信息系统、信息设备和存储设备保密管理

随着信息技术的迅猛发展，窃密活动高技术特征集中凸显，信息系统、信息设备和存储设备保密管理已成为高校科研保密管理的重中之重。

一、信息系统、信息设备和存储设备基本要求

（一）信息系统、信息设备和存储设备定义和范围

信息系统、信息设备和存储设备包含各类应用系统、服务器、计算机、网络设备、外部设施设备、存储介质、办公自动化设备、声像设备和安全保密产品。

1. 应用系统

包括由各种硬件设备及系统、接口部件、外部设备、应用软件、支持软件和工具软件组成的，为科研生产活动服务的人机系统，以及安装在信息系统中，实现某些专门应用的综合系统。

2. 服务器、计算机

包括服务器、操作终端、台式计算机、便携式计算机、工作站、小型机、中型机、大型机、巨型机等。

3. 网络设备

包括交换机、路由器、网关等。

4. 外部设施设备

包括打印机、扫描仪、移动光驱、读卡器、测试系统、调试系统、传感器系统等。

5. 存储介质

包括计算机硬盘和固态存储器、移动硬盘、光盘、U 盘、软盘等。

6. 办公自动化设备

包括打字机、复印机、传真机、多功能一体机、碎纸机、速印机、晒图机、绘图仪等，及其相关存储附件和耗材（其中部分设备也可以看作计算机的外部设备）。

7. 声像设备

包括照相机、摄像机、录音机（笔）、投影仪、专用显示器或电视机、扩音设备、存储卡、记忆棒、录音带、录像带等，及其相关附件和耗材。

8. 安全保密产品

包括单向导入、身份鉴别、访问控制、监控审计、病毒防治、恶意代码防护、干扰滤波、保密检查工具、信息消除工具等。

（二）信息设备和存储设备管理的基本要求

鉴于绝大部分高校未建立涉密信息系统，涉密信息设备与存储设备在单机环境下运行，本章将重点介绍单机环境下的信息设备和移动存储设备的保密管理。

为了确保国家秘密安全，信息设备和存储设备的管理应当遵照以下基本要求：

1. 严格遵守“涉密不上网，上网不涉密”的保密基本要求

严禁将涉密信息设备和涉密存储设备与非涉密信息设备、非涉密存储设备和非涉密信息系统、互联网及其他公共信息网络连接，或在未采取防护措施的情况下进行信息交换；严禁使用非涉密信息系统、非涉密信息设备、非涉密存储设备或未采取保密措施的有线或无线通信中存储、处理、传输国家秘密信息。

2. 严格做好涉密信息设备和存储设备“全生命周期”的管理

设备使用期间，严禁擅自卸载、修改涉密信息设备和涉密存储设备的

安全技术程序、管理程序；设备发生故障后，严禁选择不具备相应保密资格的涉密协作配套单位参与涉密信息设备和涉密存储设备的维护工作；设备不再使用后，未经安全技术处理，严禁将退出使用的涉密信息设备、涉密存储设备赠送、出售、丢弃或改作其他用途。

3. 严格控制国家秘密的知悉范围

严禁擅自存储、处理或传递知悉范围以外的国家秘密；涉密信息设备和存储设备不得存储、处理或传递高于其设备涉密等级的涉密信息；一般涉密人员不得配备、管理或者使用绝密级信息设备和存储设备；非涉密人员不得配备、管理或者使用机密级（含）以上信息设备和存储设备。

（三）管理部门职责与分工

按照“业务工作谁主管、保密工作谁负责”的原则，学校信息化管理部门是全校信息设备和存储设备的归口管理部门，负责制定管理规则与具体业务审批和管理；运行维护机构负责落实信息化管理部门的要求；保密管理机构对信息设备与存储设备的保密管理进行指导、监督和检查；设备所属单位负责日常管理。涉密设备管理的基本业务流程如图 8-1 所示。

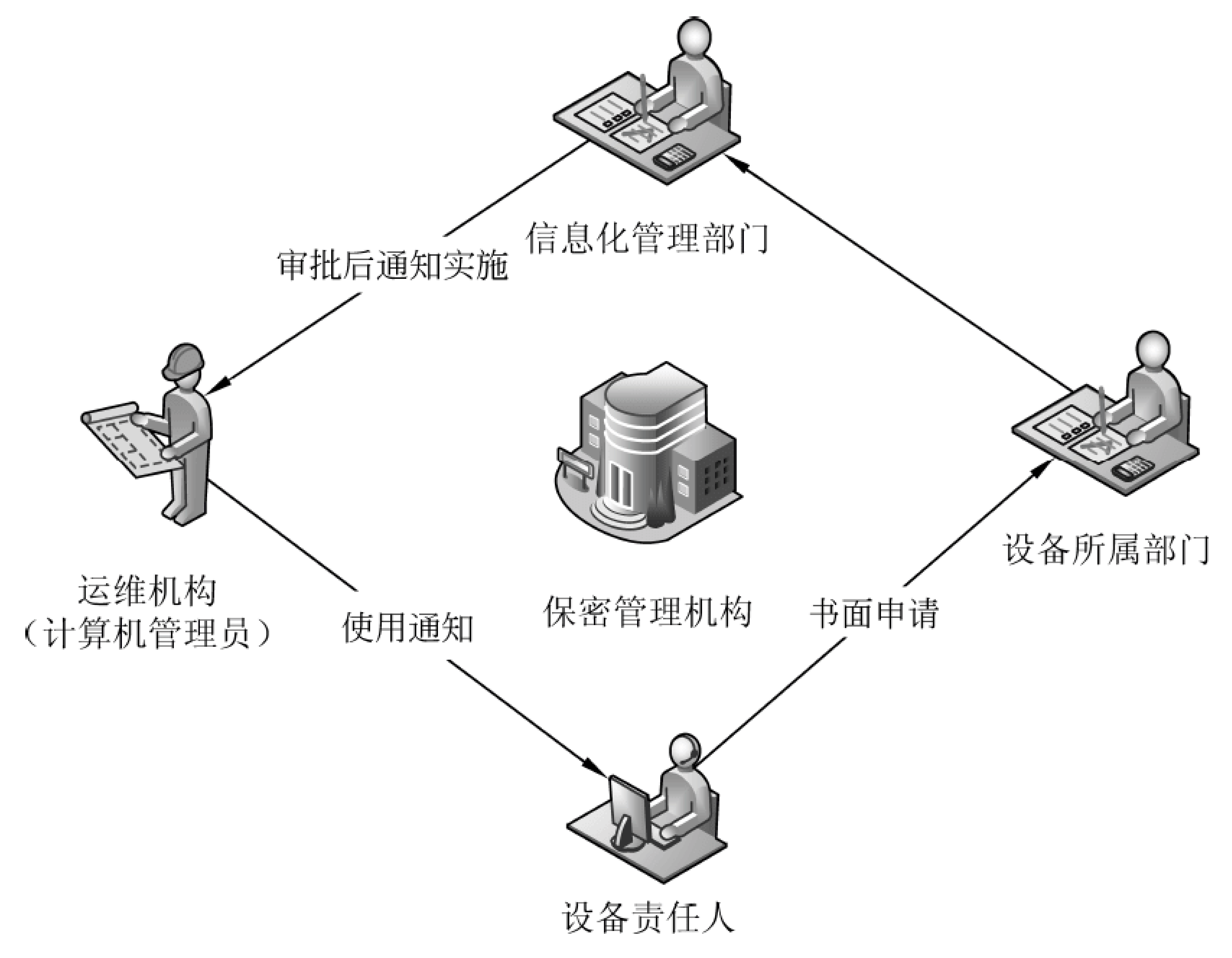


图 8-1　涉密设备管理的基本业务流程

二、涉密信息设备和存储设备全生命周期管理

（一）管理要素

涉密信息设备和存储设备管理应当形成闭环可追溯的全生命周期过程：启用前，经过严格审批并拆除不必要的设备；使用过程中，应当严格遵守相应的规章制度，严格规范开展设备使用、软硬件维护以及属性变更和检查、审计等活动；不再使用或无法使用时，设备不得随意丢弃，应当按照相应规定进行报废和销毁。

每一个涉密设备应按照生命周期建立相对应的设备档案，做到“一机一档”，图 8-2 为涉密设备的生命周期以及不同阶段的主要关注点。

（二）管理分工

涉密信息设备和存储设备全生命周期管理首先应当明确各个阶段的相关责任人和各个部门的具体分工：明确设备责任人，做到“谁使用，谁负责”；按照业务主管部门分工的不同，明确不同阶段的主管部门，做到“业务工作谁主管，保密工作谁负责”。图 8-3 为涉密设备的生命周期不同阶段管理的责任分工。

（三）涉密设备全生命周期管理基本要求

涉密设备的全生命周期在不同的使用阶段应当既符合通用性的管理要求，又重点关注关键问题，做到各阶段严格管理，确保国家秘密安全。

1．涉密设备的台账管理

《武器装备科研生产单位保密资格标准》要求建立涉密信息设备和存储设备全生命周期档案，档案应当包含设备新增、变更、维护、报废及销毁等所有审批和操作记录。学校应当建立设备的总台账，各部门应当建立相应的分台账，总台账和分台账的内容应当吻合，并与实物相符合，做到“账账相符，账实相符”。台账信息应及时更新调整，并按要求定期（绝密级 3 个月、机密级 6 个月、秘密级 12 个月）进行清查核对。

根据不同类型设备的特点，各类涉密设备台账应当记录如下相应的要素。

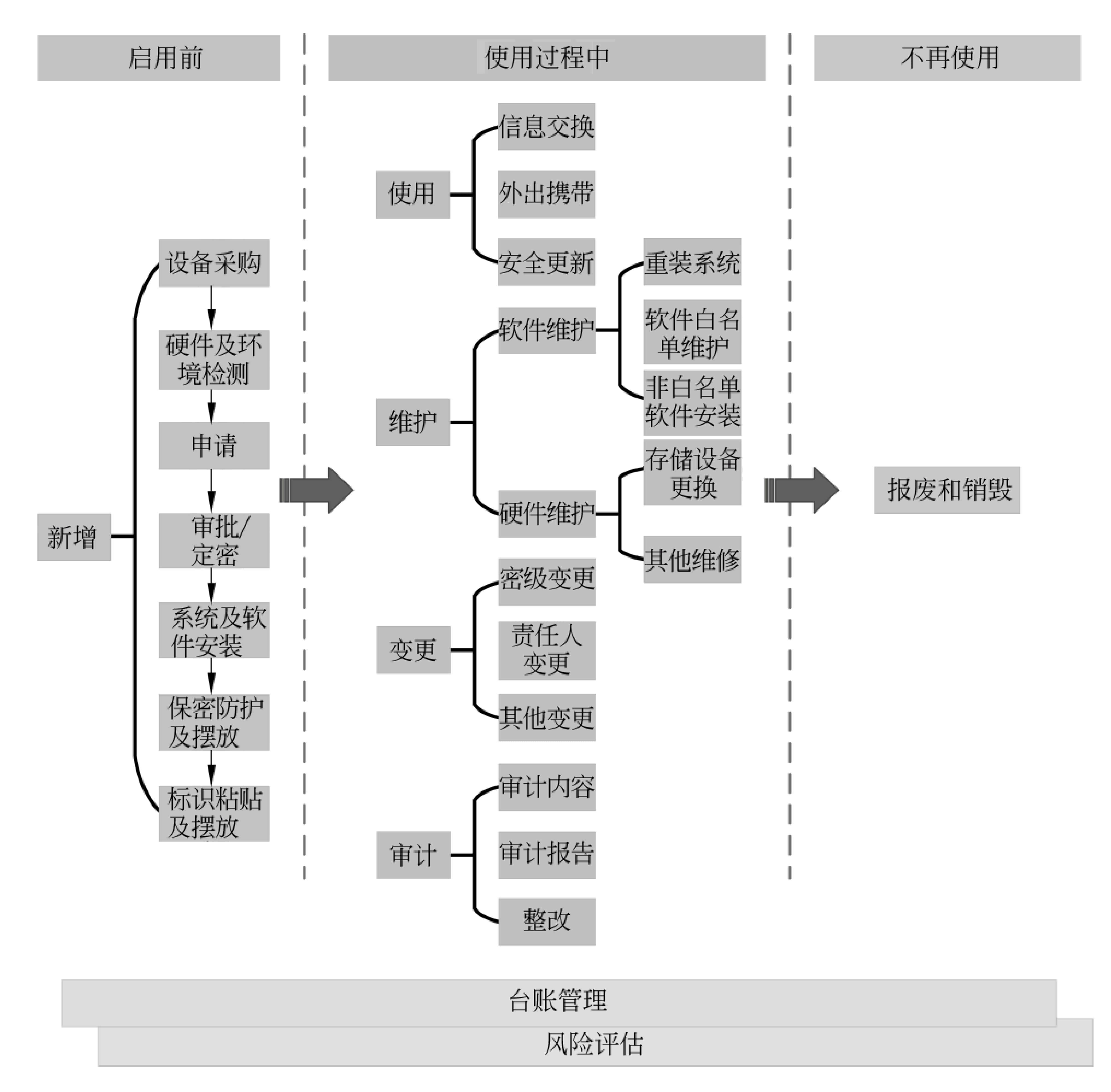


图 8-2　涉密设备的全生命周期管理示意图

（1）信息设备台账内容应包括：部门名称、设备类别、型号、保密编号、固定资产编号、设备序列号、硬盘序列号、密级、用途、MAC 地址、放置地点、责任人、使用人、设备启用时间、操作系统及版本、操作系统安装时间、安全保密产品配备、使用情况等。

（2）存储设备台账内容应包括：部门名称、设备类别、型号、保密编号、设备序列号、物理序列号、密级、用途、放置地点、设备启用时间、责任人、使用人、使用情况等。

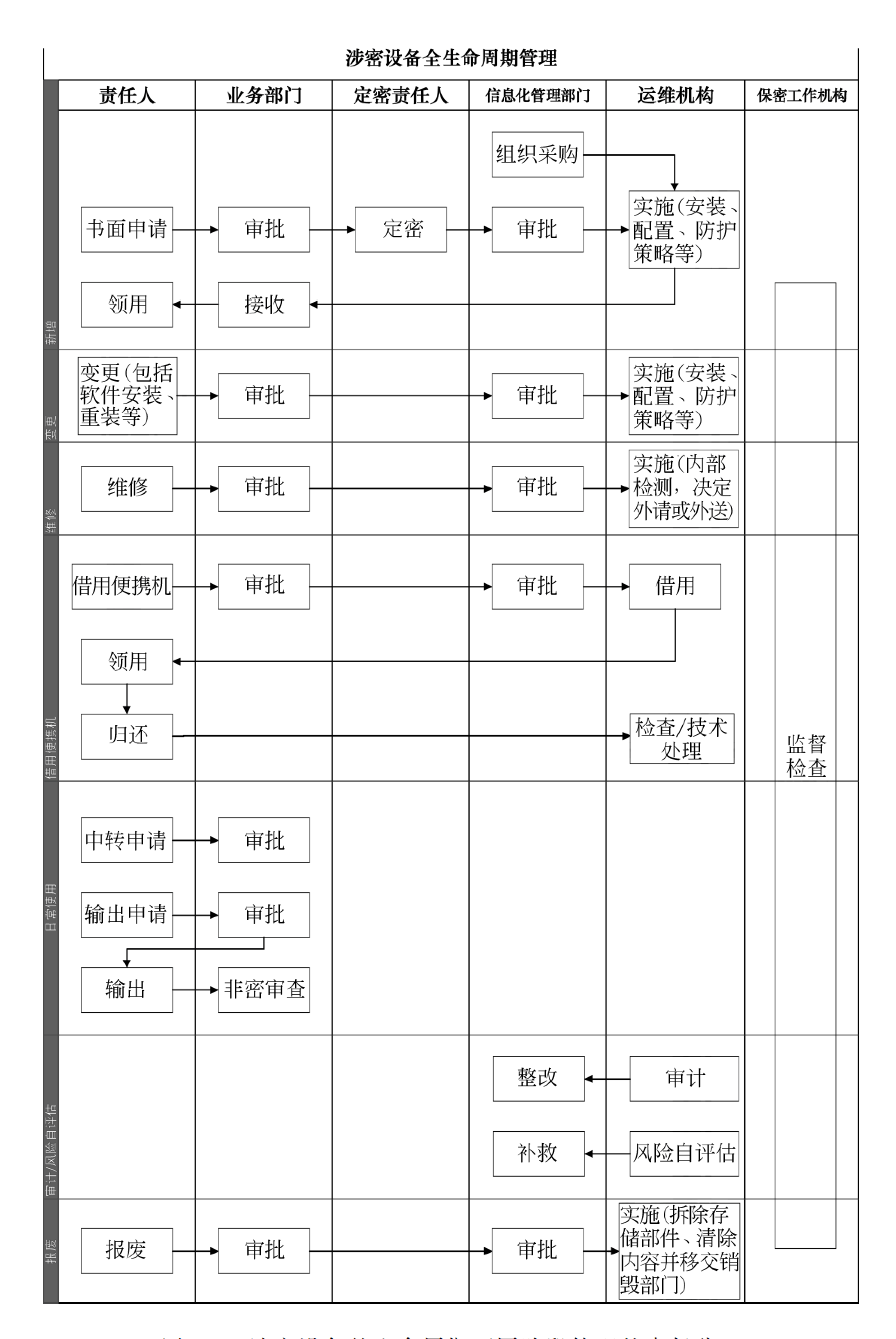


图 8-3　涉密设备的生命周期不同阶段管理的责任分工

（3）安全保密产品台账内容应包括：部门名称、设备类别、型号、生产厂家、检测证书名称、检测证书编号、购置时间、设备启用时间、保密编号、放置地点、责任人、使用情况等。

2. 新增涉密设备

新增涉密设备需要严格履行审批登记手续（参见附表 8-1），首先，由责任人根据工作需要提出申请，由相关部门对其基本条件进行审核，符合要求的申请经所在单位定密责任人定密，由运维部门对拟新增的涉密设备进行安全检查、安装操作系统和安全保密防护系统并完成相应的安全配置及系统加固，责任人办理正式领用手续后，方可正式投入使用。

3. 涉密设备场地及防辐射要求

为了防止涉密设备丢失或涉密信息被窃取，涉密设备的摆放应当满足一定的场地及防辐射要求，对于不满足条件的应当拒绝新增涉密设备的请求。

涉密信息设备应当存放在安全可靠的密闭场所内，不得放置在公共场所。涉密信息设备还应当采取一定的电磁泄漏防护措施，具体包括。

（1）涉密信息设备和导体应当满足红黑隔离要求：涉密信息设备（红设备）与非涉密信息设备（黑设备）之间应当保持规定的安全距离（一般 1 米以上，视具体情况），禁止将涉密信息设备与非涉密信息设备放置在同一个金属平台上。

（2）涉密信息设备和导体应当使用国家保密行政管理部门批准的滤波电源插座（红黑隔离电源），且一个红黑隔离电源插座上不得同时接入涉密和非涉密设备。

（3）应当采取措施对显示器等设备的电磁泄漏进行防护，如果电磁泄漏发射的安全距离超过了最小警戒距离，应当使用视频干扰仪等。

（4）涉密信息设备与发射装置（指用于广播、电视、通信等业务中的有线或无线发射设备及系统）之间应当满足隔离要求（距离 25 米以上）。

4. 涉密设备使用人员要求

用于中转和输出的涉密设备应该由具有相应涉密等级的专人管理。

工作用涉密设备(以下简称“工作机”)的使用人员,其涉密等级应当不低于涉密设备密级,即秘密级工作机使用者可以是一般涉密人员,也可以是重要涉密人员;另外,为了避免扩大国家秘密的知悉范围,除知悉范围完全相同的涉密人员,其他人不得共用涉密工作机;当设备使用者密级调整或使用人变更时,应当经信息化管理部门审批、并对设备中的数据和信息经过技术处理后方可操作,以确保使用者涉密等级与涉密设备密级匹配,且不扩大涉密设备中涉密信息的知悉范围。

5. 涉密设备硬件要求

购置不符合要求的信息设备或存储设备用于处理涉密信息,极易留下泄密隐患和信息安全风险。比如:一些计算机、加密机等电子设备设计生产商,在计算机和设备中设置“后门”,甚至隐藏了未知的无线发射设备,以便于远程监控;还有些计算机具有无线互联功能,安全性能达不到标准。因此在采购涉密信息设备时应当遵照以下要求。

(1) 按照《涉密专用信息设备采购管理规定》(财库〔2017〕165 号)的相关要求,不公开采购。

(2) 选择国家保密局《涉密专用信息设备名录》中的产品,不得选用国家保密行政管理部门禁用的设备和部件。确需采购《涉密专用信息设备名录》外产品的,应当报相关保密行政管理部门批准。

(3) 接受赠与的信息技术产品(如搜索服务器、主机、存储阵列等)一般不得用于涉密工作。确需用于涉密工作的,需要进行风险评估分析,确保受赠信息技术产品安全可靠,并报相关保密行政管理部门批准。

(4) 涉密信息设备和存储设备不能使用具有无线互联功能的设备。在使用前,必须拆除设备上具有无线互联功能的硬件模块,否则不得作为涉密设备使用。具有无线互联功能的设备不仅仅指无线网卡、蓝牙等能够实现计算机互联功能的无线设备,还包括了无线键盘、无线鼠标、红外等其他具有无线功能的设备。

另外,涉密信息设备使用前,应当提请运维部门或指定的技术部门进行专门的安全保密技术检测,确认不存在泄密风险和安全隐患后再用于处

理涉密信息。涉密信息设备使用中，禁止擅自安装、拆卸、更换硬件设备，应当使用物理防护措施（如易碎封条或带锁的机箱保护外壳等）对机箱进行控制。

6. 涉密计算机安全配置及系统加固

涉密计算机必须设置 BIOS 管理口令、BIOS 开机启动口令、操作系统登录口令，并在 BIOS 中关闭不必要的功能（如选择启动设备、多余端口等）。BIOS 管理口令应当由计算机安全保密管理员管理，BIOS 开机启动口令和操作系统登录口令由用户设定。设置密码应当遵循以下规则。

（1）处理秘密级信息，口令长度不得少于 8 个字符，更换周期不得长于一个月。

（2）处理机密级信息，口令长度不得少于 10 个字符，更换周期不得长于一周。

（3）处理绝密级信息，采用一次性口令或生理特征等强身份鉴别措施，口令长度不得少于 12 个字符，采用大小写英文字母、数字和字符中两者以上的组合。

（4）登录涉密计算机操作系统和应用系统须进行身份鉴别，身份鉴别成功后空闲操作时间超过规定值（不超过 10 分钟），须重新进行身份鉴别。当身份鉴别尝试失败次数达到 3 次时，须对用户进行锁定，同时形成审计事件并告警，且只能由计算机安全保密管理员恢复。

涉密计算机安装的操作系统应当通过修改安全配置、增加安全机制等方法进行加固，合理进行安全性加强。加固内容包括打补丁、文件系统、账号管理、网络及服务、注册表、共享、应用软件、审计/日志及其他（包括紧急恢复、数字签名等）。

涉密计算机必须安装符合国家保密要求的安全防护产品，安装审计软件对用户行为进行审计并设置合理的安全策略。安全策略的设置原则为：关闭所有不必要的端口、共享、服务、链接、系统授权及光驱、打印等权限，根据实际情况仅开放所必须的端口。实际情况需要开放端口的，需经信息化管理部门审批后有限制地开放。

涉密计算机必须统一安装符合要求的国产防病毒软件，并定期（不超过15天）升级病毒库，每次更新病毒库后需要对系统做一次全面查杀。涉密计算机应当及时安装操作系统、数据库和应用系统的补丁程序（在补丁程序发布后3个月内）。

涉密计算机上不得随意安装软件，不得安装国家保密行政管理部门禁用的软件，尽量使用具有相同功能的国产软件。应根据实际需要编制“涉密计算机软件白名单”，并在信息化管理部门审批备案。安装白名单内的软件不需要审批；安装非白名单内的软件，需要进行申请，经信息化管理部门批准后方可操作。当“涉密计算机软件白名单”发生变化时，需要重新审批备案。“涉密计算机软件白名单”应当包括软件名称、版本、用途及使用范围几个要素。可以提前将软件刻录光盘或导入涉密计算机备用，但软件刻录或导入前需要进行病毒和恶意代码查杀。

7. 标志粘贴及摆放

涉密设备必须粘贴标识，标明保密编号、密级和保密责任人信息，并在明显位置粘贴安全警示信息。

涉密计算机的显示器、投影仪等显示设备和键盘等输入设备应采取适当的遮挡措施，不应面对门窗、安防监控系统及其他可能被窥视的方向摆放。

（四）涉密设备的变更

涉密设备的使用部门、责任人、使用人、密级、存储设备、放置地点等发生变更时，需经信息化管理部门批准后实施变更（参见附表8-2），并根据实际情况（如知悉范围发生变化或密级降低等）决定是否对硬盘或其他存储介质上的数据进行技术处理（如擦除数据等）。

涉密设备在一段时间内不使用，需要将设备使用状态及时变更为停用状态。经信息化管理部门批准后，由计算机安全保密管理员拆除硬盘等存储介质，并封存在保密柜内。

（五）涉密设备的系统维护

严禁擅自对涉密计算机和信息系统进行格式化或重装操作系统，严禁擅自删除移动存储介质及外部设备等日志记录。

因系统崩溃、操作系统损坏等原因确需重装操作系统时，需经信息化管理部门审批后，由运行维护机构重新安装系统。

因特殊情况需要删除移动存储介质及外部设备等日志记录时，需详细说明具体原因，经信息化管理部门审批后，由运行维护机构实施。

因特殊情况需要对硬盘或其他存储介质的数据进行清除时，需说明具体原因，经信息化管理部门批准后，对硬盘或其他存储介质进行数据擦除。擦除后的硬盘或其他存储介质，如果保存过涉密信息，不得再作为非密存储介质使用。

（六）涉密设备的维修

涉密计算机和外部设备、存储介质发生故障需维修时，需详细说明故障情况，经信息化管理部门批准后方可进行维修，维修后须详细记录维修情况并进行保密检查。

涉密设备现场维修一般由内部维修人员维修。由外部人员到现场维修时，需选择信息化管理部门指定的具备涉密信息设备和涉密存储设备维护工作保密资格的涉密协作配套单位，且维修过程必须由专人全程旁站陪同，禁止维修人员恢复、读取和复制被维修设备中的涉密信息。

涉密设备需要带离进行维修的，应当拆除所有存储过涉密信息的硬件和固件，送到指定维修地点并与维修单位和维修人员签订保密协议。如果涉密设备中存储过涉密信息的硬件和固件不能拆除或涉密存储硬件和固件发生故障时，应当送至具有涉密信息系统数据恢复资质的单位进行维修，或者按照涉密载体销毁要求进行销毁。

（七）涉密设备内存储文件的要求

涉密信息设备和存储设备中产生、处理、传输和存储的各类涉密文档、

图表、图形、图像、音频、视频及其他数据文件等，应当依据其内容准确标注密级，及时清理、备份及归档，并遵循以下原则。

（1）处于起草、设计、编辑、修改过程中和已完成的电子文档、图表、图形、图像、数据，如涉及国家秘密，应当在首页按照相关规定准确标注密级与保密期限，并将密级标识作为文件名称的一部分进行标注。

（2）电子数据文件、图表、图形、图像、音频等涉密信息在首页无法直接标注密级的，将密级标识作为文件名称的一部分进行标注。

（3）涉及国家秘密的软件程序、数据库文件、数据文件、视频文件等，在软件运行首页、数据视图首页和影像播映首页标注密级；如果可能，则将密级标识作为文件名称的一部分进行标注。

（4）涉密计算机内存储的相关涉密文档、图表、图形、图像、音频、视频及其他数据文件应当按照涉密科研项目对资料归档的要求，在项目结题验收阶段及时进行清理，删除不再需要的临时文件或中间数据，将具有保存价值的资料进行归档。清理后由计算机安全保密管理员采取有效的技术手段对保存过涉密信息的设备及存储介质进行处理，确保已删除的数据不可再恢复。

（5）归档资料应当按照输出控制的要求进行审批登记，标明密级、保密期限等信息，由各涉密二级单位集中管理或移交学校档案管理部门归档保存，其中重要的数据可以采用多种不同的存储介质进行保存（如同时使用纸介质和光盘保存）。

为了确保落实以上要求，各涉密二级单位或课题组应当明确专人负责电子信息归档的组织、管理和监督检查。

（八）涉密设备报废

不再使用或长期停用的涉密设备应当及时做报废处理。

涉密设备需要报废时，需报学校信息化管理部门审核（参见附表 8-3）。设备中具有存储功能的硬件和固件，删除其中的涉密信息后，上交学校信息化管理部门统一进行技术处理后，留作涉密用途使用或集中送交具有保

密资质的销毁中心进行物理销毁。涉密设备其他硬件和固件报废可按仪器设备报废的有关规定执行，无法拆除具有存储功能的硬件和固件的应当整机销毁。

禁止将涉密计算机作为废品出售；如用作捐赠时，须更换硬盘等具有存储功能的硬件。存储过涉密信息的硬件和固件进行技术处理后，不得作为非密存储设备使用。

（九）涉密设备遗失

涉密设备一旦遗失或下落不明，应当立即报告学校信息化管理部门和保密管理部门，必要时可提请公安部门及上级保密管理部门协助。按照相关规定要求，涉密设备自发现丢失之日起，绝密级 10 日内或机密、秘密级 60 日内查无结果的，按泄密事件处理。

三、特定涉密设备的管理要求

（一）涉密计算机保密管理要求

除了涉密设备全生命周期管理的通用要求，涉密计算机在使用中还应当遵循以下原则。

（1）涉密计算机应当安装正版操作系统，并安装统一配发的各类监控、审计、杀毒、恶意代码防护等安全保密防护系统；禁止擅自卸载防护及监控系统，禁止在未经审批的情况下修改防护及监控系统配置。

（2）涉密计算机应当按要求进行安全设置和加固，并使用符合要求的身份鉴别措施。

（3）涉密计算机责任人应当妥善保管相关密码及 USBKey，未经审批，禁止将涉密计算机授权他人使用。

（4）涉密计算机应当定期安装操作系统和应用程序补丁、更新病毒和恶意代码防护产品特征库，并进行病毒及恶意代码的全盘查杀、清除病毒隔离区；未经学校信息化管理部门审批，用户不得擅自安装补丁和更新特

征库。

（5）禁止擅自安装、拆卸涉密计算机上的软件。应当根据自身的需求设定软件白名单并报学校信息化管理部门，经审批后安装白名单内的软件需进行记录，若安装白名单之外的软件则需履行相关的审批手续。

（6）涉密计算机只能用于处理、存储与自身密级相符的涉密信息，严禁处理、存储比自身密级更高的信息。

（7）涉密计算机中存储的各类涉密电子文档、图表、图像、数据、声像等资料应按规定标明密级和保密期限。

（8）涉密计算机中的信息导入、导出应相对集中，并按照规定的流程进行审批、操作及记录。

（9）涉密计算机应当按规定的周期进行审计及自查，并根据审计日志及自查结果形成审计报告及自查报告；对于审计及自查中发现的问题要及时采取补救措施并报告学校信息化管理部门。

（二）涉密外部设施设备保密管理要求

涉密外部设施设备是指需要连接涉密计算机的打印机、扫描仪、外接刻录设备、读卡器等信息设备，除了涉密设备全生命周期管理的通用要求，在使用过程中还应当遵循以下原则。

（1）涉密外部设施设备应当根据其处理的涉密信息的最高密级来确定自身的密级。

（2）涉密外部设施设备原则上需绑定到指定的涉密计算机上使用，严禁接入非涉密计算机或密级低于自身密级的涉密计算机上使用。

（3）通过 USB 口连接计算机的涉密外部设施设备应当记录其在计算机中的唯一序列号，并将相关序列号体现在台账中。

（4）涉密外部设施设备在处理、输入及输出信息时应当按规定要求履行审批手续，并做好记录。

（三）涉密存储设备保密管理要求

涉密存储设备是指用于存储涉密信息的 U 盘、移动硬盘、光盘等存储

介质，除涉密设备全生命周期管理的通用要求外，在使用过程中还应遵循以下原则。

（1）涉密存储设备应当按其存储信息的最高密级进行定密；涉密人员应根据其岗位密级配备相应密级的涉密存储设备，并在授权的设备上使用。

（2）涉密存储设备应当指派专人集中管理，并根据涉密等级存放在相应的保密柜（或密码保险柜）等符合国家保密要求的设备设施中。

（3）借用涉密存储设备时应当履行审批程序，用后及时归还；禁止在低密级计算机及信息设备上使用高密级存储介质，禁止在低密级存储介质上存储高密级信息。

（四）涉密办公自动化设备和涉密声像设备保密管理要求

涉密办公自动化设备是指复印机、打字机、传真机、多功能一体机、碎纸机、速印机、晒图机、绘图仪等无须连接计算机即能独立使用的信息设备，涉密音像设备指照相机、摄像机、录音机、录音笔、投影仪、非线性编辑机、扩音设备、音频矩阵、视频矩阵、视频会议设备、数字化会议设备、存储卡、记忆棒、录音带、录像带等用于音像采集和处理的信息设备，除了涉密设备全生命周期管理的通用要求，在使用过程中还应当遵循以下原则。

（1）涉密办公自动化设备和涉密声像设备应当明确用途并指派专人进行管理和使用，设备的使用情况应当完整记录。

（2）如涉密办公自动化设备和涉密声像设备有存储功能，其存储部件应当按涉密存储设备进行管理。

（3）涉密办公自动化设备和涉密声像设备处理的信息需按照有关规定履行相关的审批登记手续。

（五）涉密安全保密产品保密管理要求

涉密安全保密产品是指单向导入、身份鉴别、访问控制、监控审计、病毒防治、恶意代码防护、干扰滤波、保密检查工具、信息消除工具等用于安

全保密防护和具有安全保密功能的信息设备，除了涉密设备全生命周期管理的通用要求，在使用过程中还应当遵循以下原则。

（1）应当选用获得国家相关主管部门批准的国产产品；查验产品与检测报告和证书一致，并在有效期内。

（2）按照要求进行管理、部署、使用和策略配置，并确保正常使用，未经学校信息化管理部门批准不得变更。

（3）学校信息化管理部门每半年对安全保密产品的部署情况、策略设置和工作状态进行检查并记录。安全保密产品发生故障时应当及时维修，不能维修的应做技术更换，确保安全保密产品处于正常的工作状态。

（六）便携式涉密信息设备和存储设备保密管理要求

由于便携式涉密信息设备和存储设备的易携带性，为降低其失泄密风险，按照《武器装备科研生产单位保密资格审查认定管理办法》要求，应当根据工作需要配备专供外出携带和内部使用的便携式涉密信息设备和存储设备。这类设备除应当按涉密信息设备和存储设备相关操作规程要求使用外，在使用过程中还应当遵循以下原则。

（1）专供外出携带涉密信息设备和存储设备，应当由学校运行维护机构负责集中管理和维护，一般不得在学校内部使用，并履行严格的使用登记和保密检查制度。确因特殊情况需要在学校内部使用的，需报学校信息化管理部门审批。

（2）供内部使用的涉密便携式涉密信息设备和存储设备按照要求集中管理，不得带出学校，并执行使用登记制度；确因特殊情况需要携带外出的，需经学校信息化管理部门审批，并由运行维护机构进行保密检查和数据清除。

外出携带涉密信息设备和存储设备，应当按以下要求进行管理和使用。

（1）携带涉密信息设备和存储设备外出前，应经学校信息化管理部门审批后（参见附表 8-6），方可借出使用；学校运行维护机构在涉密信息设备

和存储设备借用外出前进行保密检查。

（2）借用人应确保携带外出的涉密信息设备和存储设备中仅存有与本次外出工作有关的涉密信息，并在归还前将相关信息进行清除，严禁清除系统区以及各类系统日志和安全产品日志文件。

（3）外出期间，借用人对携带外出的涉密信息设备和存储设备负有保密管理责任，按保密要求严格管理，并详细记录设备的使用情况。

（4）归还后运行维护机构应当与借用人共同进行保密检查，并进行必要的信息清除，确保涉密数据不可恢复。

（七）涉密专用设备保密管理要求

在科研工作中常常会有一些用于测试、调试、仿真、工控、数控等特殊用途的专用涉密信息设备，以及无法安装安全保密产品或安装后影响使用的涉密计算机，这些设备被统称为涉密专用设备。由于这些专用设备无法安装相应的安全保密产品，在使用过程存在较大的失泄密隐患，应当遵循以下原则。

（1）涉密专用设备应当根据工作需要明确涉密等级，指定责任人负责管理和维护。

（2）涉密专用设备应当做物理封堵或拆除不使用的网络、USB、串行、并行、读卡器等数据接口，充分利用操作系统提供的功能进行安全策略配置，并定期检查其安全状态。

（3）涉密专用设备应当安装相应的安全保密产品、设置相应的安全策略；无法安装安全保密产品，或安装后影响设备正常使用的，应说明理由提出申请，经学校信息化管理部门批准后可不安装。使用中应加强管理，制定专项管理制度、安全保护策略和技术控制措施。

（4）涉密专用设备的维修、报废和销毁按照涉密设备的要求执行。

（5）涉密专用设备与涉密信息设备和存储设备之间的信息交换应采取单向方式，导入和导出应采用不同的端口，或通过“三合一”的非涉密信息交换口单向导入。

（6）涉密专用设备独立构成涉密网络的，应按涉密信息系统分级保护的要求，申请涉密信息系统的系统测评（风险评估），取得国家保密行政管理部门颁发的《涉及国家秘密的信息系统使用许可证》。

四、涉密信息交换

高校科研工作离不开信息交换，信息交换过程存在着外来恶意信息的导入、内部涉密信息的非法输出、违规交换导致知悉范围扩大等一系列的失泄密隐患，是涉密信息设备和存储设备保密管理的重点工作之一。

涉密信息交换是指涉密信息设备与外部的信息交换，包括涉密信息的导出、外来涉密信息和非涉密信息的导入，以及单位跨部门内部涉密单机间信息的交换。因涉密信息设备不连接互联网，同时，为了避免针对移动存储设备的跳板攻击，涉密信息交换应当通过专用的设备进行，遵循相对集中、专人管理的原则，并严格履行审批登记手续、控制信息的流向。

（一）外来信息导入

外来信息是指来源于校外的信息。根据拟导入信息的密级不同，外来信息导入应当分别通过涉密中间机（涉密信息导入）、非涉密中间机或单向导入设备（非涉密信息导入）进行。

中间机是指与其他任何计算机和信息系统实行物理隔离、独立运行的专用计算机，主要用于将外来信息导入到内部涉密信息设备和存储设备中。根据导入数据的类型不同，中间机分为用于导入涉密信息的涉密中间机和用于导入非涉密信息的非涉密中间机（或单向导入设备）。

涉密中间机按涉密计算机管理，密级按其处理的涉密信息的最高密级确定，须安装指定的主机监控和审计系统，并安装与其他涉密计算机不同的防病毒软件；涉密中间机仅用于信息交换，不得用于信息处理。非涉密中间机为不联网的非涉密计算机，安装必需的防护软件和刻录光驱，对数

据接口进行适当控制。

外部涉密信息导入涉密计算机时，只允许使用一次性只读光盘通过涉密中间机导入。导入时需要先将外部信息从光盘拷贝到涉密中间机上，对所拷贝信息进行杀毒后，再转存到内部使用的涉密中转存储介质上，在涉密计算机上读取。导入完成后，须删除在涉密中间机和中转涉密存储介质上临时存储的信息，并采取技术措施确保数据不会被恢复。

外部非涉密信息（电子文档）导入涉密计算机时，应当经非涉密中间机刻录一次性只读光盘的方式或使用单向导入设备导入，严禁直接读取非涉密光盘。

图 8-4 为外来信息导入的参考流程。

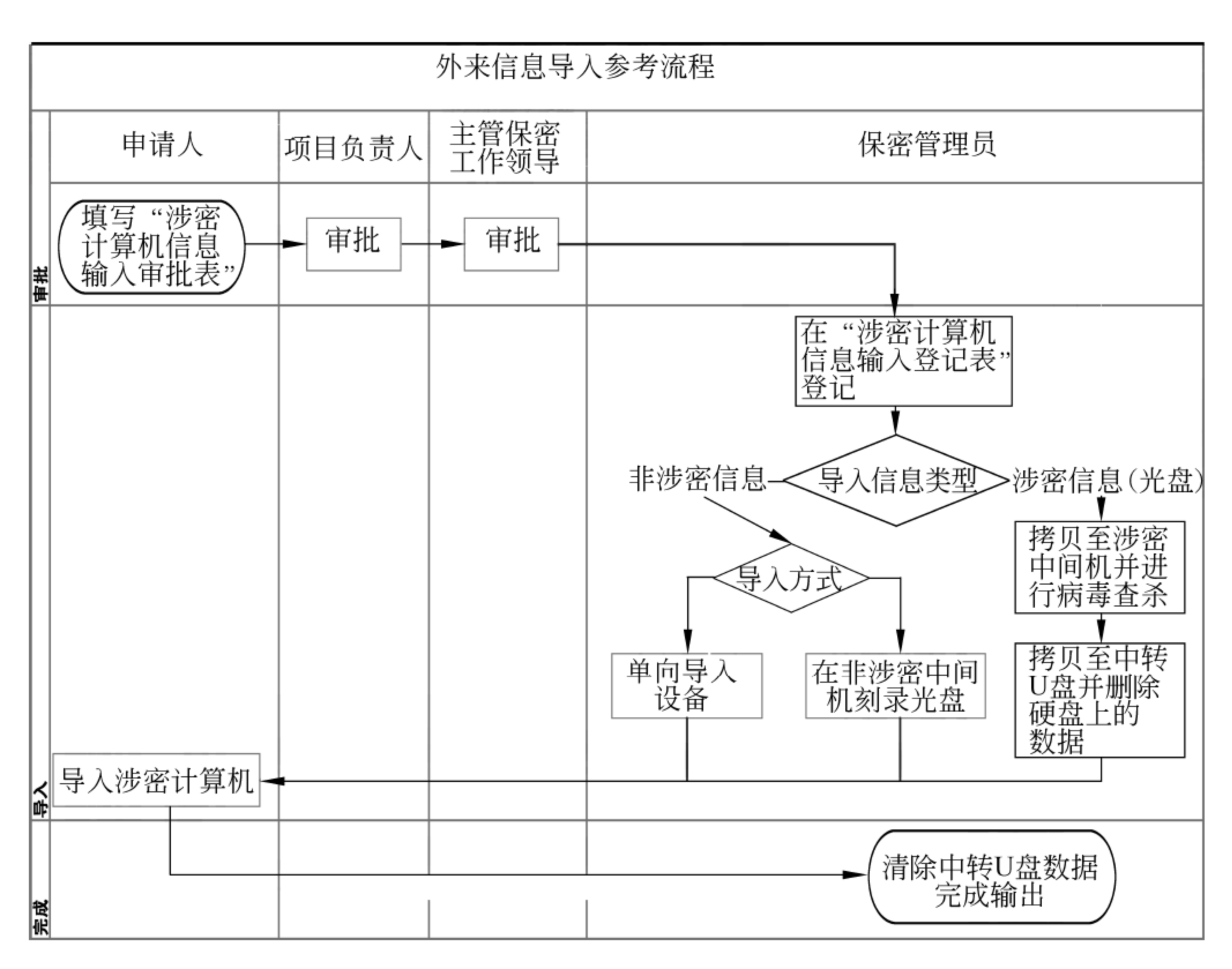


图 8-4　外来信息导入参考流程

外来信息导入前需要经过主管领导批准；操作过程应当详细登记操作

人、操作时间、导入的文件内容等(参见附表 8-4)。

(二)信息导出

涉密输出机是指具备输出功能(打印/刻录)的涉密计算机,学校应当设置固定的涉密信息集中输出点,由专人负责管理,并在输出过程中严格履行审批登记手续。

涉密计算机中的信息导出时,一般应当输出纸介质文件;确因工作需要以电子文件输出信息时,应当采取刻录一次性只读光盘的方式进行输出。图 8-5 为信息导出的参考流程。

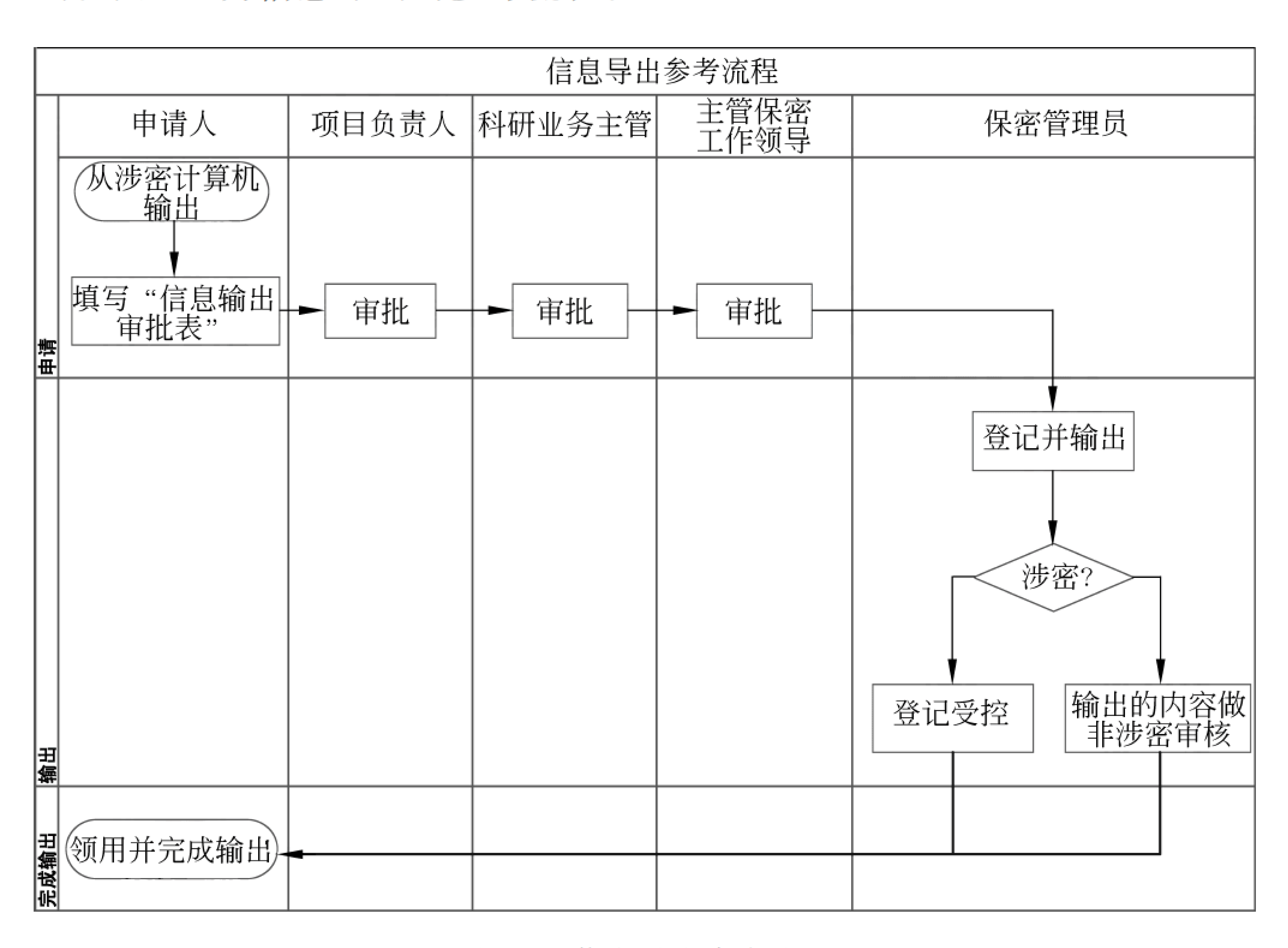


图 8-5 信息导出参考流程

导出信息必须严格遵循先审批再输出的要求操作(参见附表 8-5),经过项目负责人和所在单位保密主管领导批准后才可以输出;导出时,应当登记申请人、操作人、输出时间、输出内容及数量等信息;操作人应当审核

输出的内容与申请登记的内容一致；输出的非涉密信息，信息载体（文件、光盘等）须经所在单位保密负责人或经其授权的审核人对内容进行非密信息审核后，方可交给申请人使用；输出的涉密信息，信息载体（文件、光盘等）应严格遵循涉密载体保密管理的要求进行登记和管理。

（三）学校内部信息交换

高校涉密科研使用的主要是涉密单机，应当通过安全可靠的渠道进行学校内部涉密机之间的信息交换。一般应当通过涉密专用 U 盘、移动硬盘或涉密光盘进行信息交换。

涉密光盘由于其在传递、使用过程中的安全隐患较大，导出、导入的过程需要履行登记受控以及用后销毁等相关手续，使用的过程比较烦琐。

涉密专用 U 盘/移动硬盘由于可以通过绑定、授权等技术措施限定其使用范围，是最常用的内部信息交互介质。

为了避免知悉范围的扩大，涉密专用 U 盘/移动硬盘应当根据其使用范围不同进行区分，一般包括责任人个人专用、单位内部中转专用、单位内部输出专用、外出携带专用。

（1）个人用涉密 U 盘只做个人备份数据或相同责任人的多个工作机之间信息交换使用，不得用作输出、中转和外出携带。

（2）涉密中转 U 盘除承担将涉密中间机中的数据中转到个人工作机上的功能外，还承担了内部信息中转的功能（通过不同涉密中间机进行），授权使用范围为个人工作机、所有涉密中间机上使用。

（3）涉密输出 U 盘用于将要导出的文件从个人工作机上拷贝至涉密输出机上输出，授权使用范围为个人工作机、涉密输出机上使用。

（4）涉密便携 U 盘用于将工作文件从个人工作机上拷贝至涉密便携机上使用，授权使用范围为个人工作机和便携机。

图 8-6 所示为不同类型 U 盘/移动硬盘的使用范围参考。

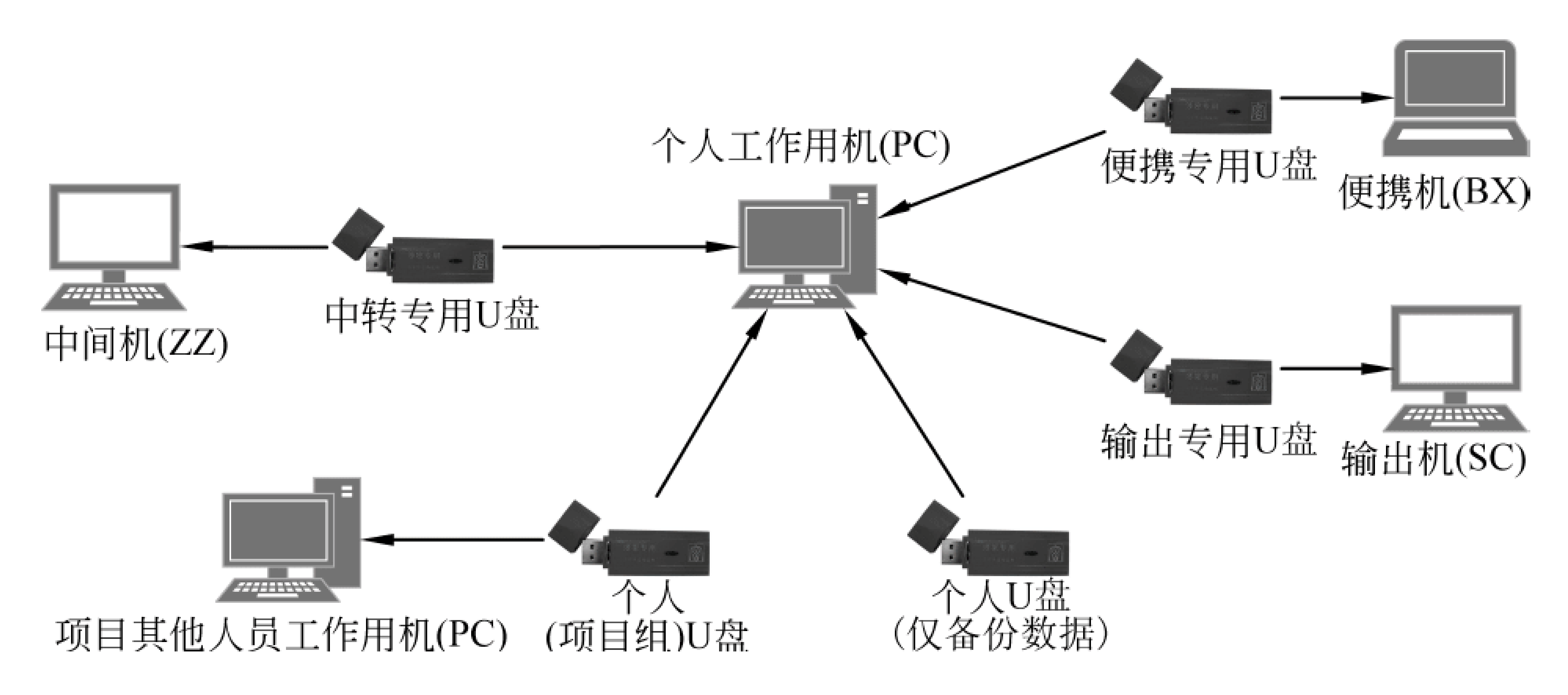


图 8-6　涉密 U 盘分类及使用范围参考

五、非密信息系统、信息设备和存储设备的保密管理

（一）非涉密信息系统、信息设备和存储设备基本要求

非涉密信息系统、信息设备和存储设备应当按“控制源头、加强检查、明确责任、落实制度”的原则进行管理。严禁在非涉密信息系统、信息设备和存储设备上传输、存储和处理涉及国家秘密信息，禁止在连接互联网的非涉密信息系统、信息设备和存储设备上传输、存储和处理国防项目、课题相关的敏感信息和内部信息。

非涉密信息设备和存储设备应当按照要求建立台账，并指定专人进行维护和管理，定期清查核对。非涉密信息系统，应当坚持“谁上网谁负责”的保密原则，相关责任人签订保密协议，并由信息系统的责任人做好内容审查和保密检查。

非涉密信息设备和存储设备还应当遵循以下规则。

（1）在涉密场所使用的非涉密计算机不得安装、配备和使用摄像头和麦克风等视频、音频输入设备。

（2）涉密人员使用的非涉密计算机或在涉密场所使用的非涉密计算机应严格遵照单位信息化管理部门统一要求安装操作系统、杀毒软件及相关办公软件。更改计算机硬件配置或重装操作系统须及时通知本单位计算

机保密管理员更新台账，禁止擅自停用或卸载杀毒软件。

（3）非涉密计算机禁止安装和使用非正版软件。

（4）连接互联网的非涉密信息设备责任人应当对终端的使用和信息导入导出情况负责。如需要从国际互联网或其他公共信息网络下载信息、程序和软件工具时，下载后应当先查杀木马和病毒，再安装及使用。工作用非涉密计算机禁止私自导入与工作无关的信息和软件。

（5）不要随意打开陌生的链接或下载、安装来源不明的软件。不得将来源不明的存储介质接入工作用非涉密计算机。

（6）涉密人员发现计算机遭到来源不明的攻击，应当及时断开网络并上报本单位的计算机安全保密管理人员记录，对于严重的攻击行为应当提交到保密管理部门及信息化管理部门处理。

（7）不应当将未登记的信息设备和存储设备处理带到工作场所，或使用未登记的信息设备和存储设备处理工作信息。

（8）手机、移动终端等移动通信设备和非涉密信息设备不得连接涉密信息设备使用的红黑隔离电源。

（二）非涉密信息设备和存储设备台账

由于高校的特殊性，无法将所有非涉密信息系统、信息设备和存储设备纳入台账管理，单位最低限度应当将涉密人员使用的或在涉密场所使用的信息设备和存储设备纳入台账管理的范围。其中，包括不在涉密人员名下，但涉密人员需要使用的设备，如网络共享打印机、复印机、扫描仪等，对于多人共用的非涉密信息设备和存储设备还应当明确责任人。

根据不同类型设备的特点，非涉密设备台账应当记录如下相应的要素。

（1）非涉密计算机台账内容应包括：部门名称、设备类别、型号、固定资产编号、设备序列号、硬盘序列号、用途、MAC 地址、IP 地址、放置地点、责任人、使用人、操作系统及版本、操作系统安装时间等。

（2）非涉密存储设备台账内容应包括：部门名称、设备类别、型号、编

号、USB序列号、用途、放置地点、责任人等。

（3）非涉密外部设施设备台账内容应包括：部门名称、设备类别、型号、固定资产编号、USB序列号、用途、放置地点、责任人等。

（4）非涉密办公自动化设备台账内容应包括：部门名称、设备类别、型号、固定资产编号、设备序列号、存储固件序列号、用途、放置地点、责任人等。

（5）非涉密声像设备台账内容应包括：部门名称、设备类别、型号、固定资产编号、设备序列号、物理序列号（根据设备不同填写能够唯一区分的序列号）、用途、放置地点、责任人等。

各部门应当建立本单位的非涉密信息设备和存储设备台账，定期汇总到学校形成单位的总台账。台账应及时更新调整，与实物相符合，做到"账账相符，账实相符"，并按要求定期（不低于12个月）进行清查核对。

（三）非涉密信息系统和信息设备技术防范措施

高校非涉密信息系统、信息设备包括校园内和校园外两种环境，校园内由校园网、数据中心和非涉密计算机终端组成，校园外主要指微博、微信、博客等公共网络媒体，不同环境面临的安全威胁不同，需要采取的安全保密措施也不相同。通常可在传统的防火墙、防病毒、漏洞检测等防护手段的基础上，增加信息发布的内容审查、互联网信息的内容审计、非涉密计算机终端监控审计等保密防护手段，形成高校非涉密信息系统和信息设备的保密技术方案，如图8-7所示。

1. 互联网应用外发审查

据教育部不完全统计，高校的互联网泄密事件类型有95%以上来自网站信息泄密和邮件泄密。而高校的传统防护手段多以事后审计追责为主，网站信息发布、公文发布、邮件系统等重要信息发布平台缺少保密监控审查机制，导致涉密信息无意识外发。为防范此类的安全风险，可部署互联网应用外发审查系统。

互联网应用外发审查的典型架构如图8-8所示。

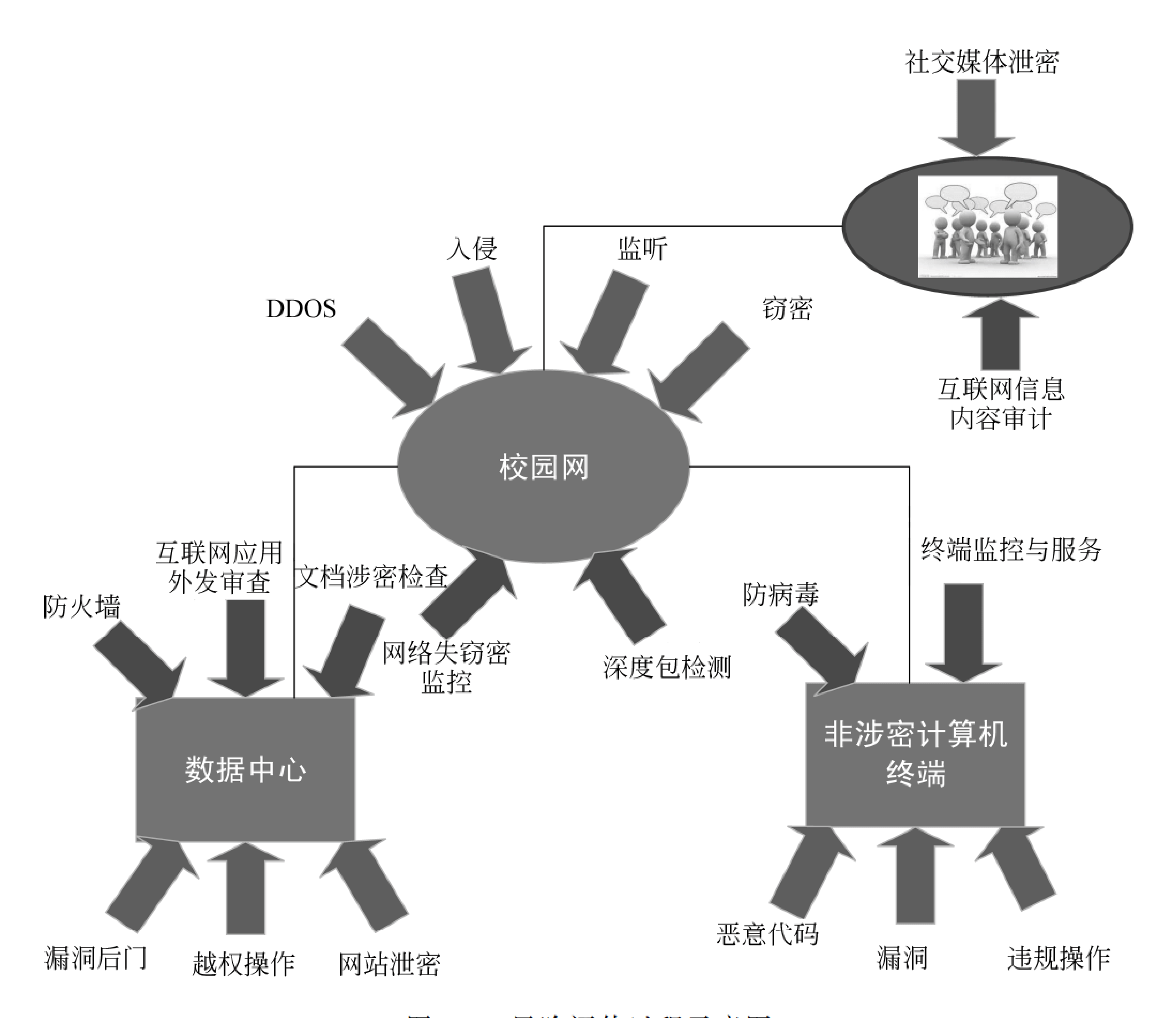


图 8-7　风险评估过程示意图

当用户使用应用系统进行信息发布时(如网站信息发布或邮件外发),应用服务器自动将发布内容提交至检测服务器进行保密审查。检测服务器审查完成之后策略管理中心会记录审查结果,检测器会将审查结果(通过或不通过)反馈给应用服务器,应用服务器将“不通过”的审查结果反馈给用户,将“通过”的审查结果直接进行发布。

网站信息发布属强制检查,检查未通过无法进行下一步流转。其中,基础策略库由主要业务管理部门合作完成,避免因单位性质不同导致的漏审核;终端用户可进一步确认文档是否涉密,降低了因缺少保密审核带来的泄密风险,也降低“二级领导”行政审核的风险。

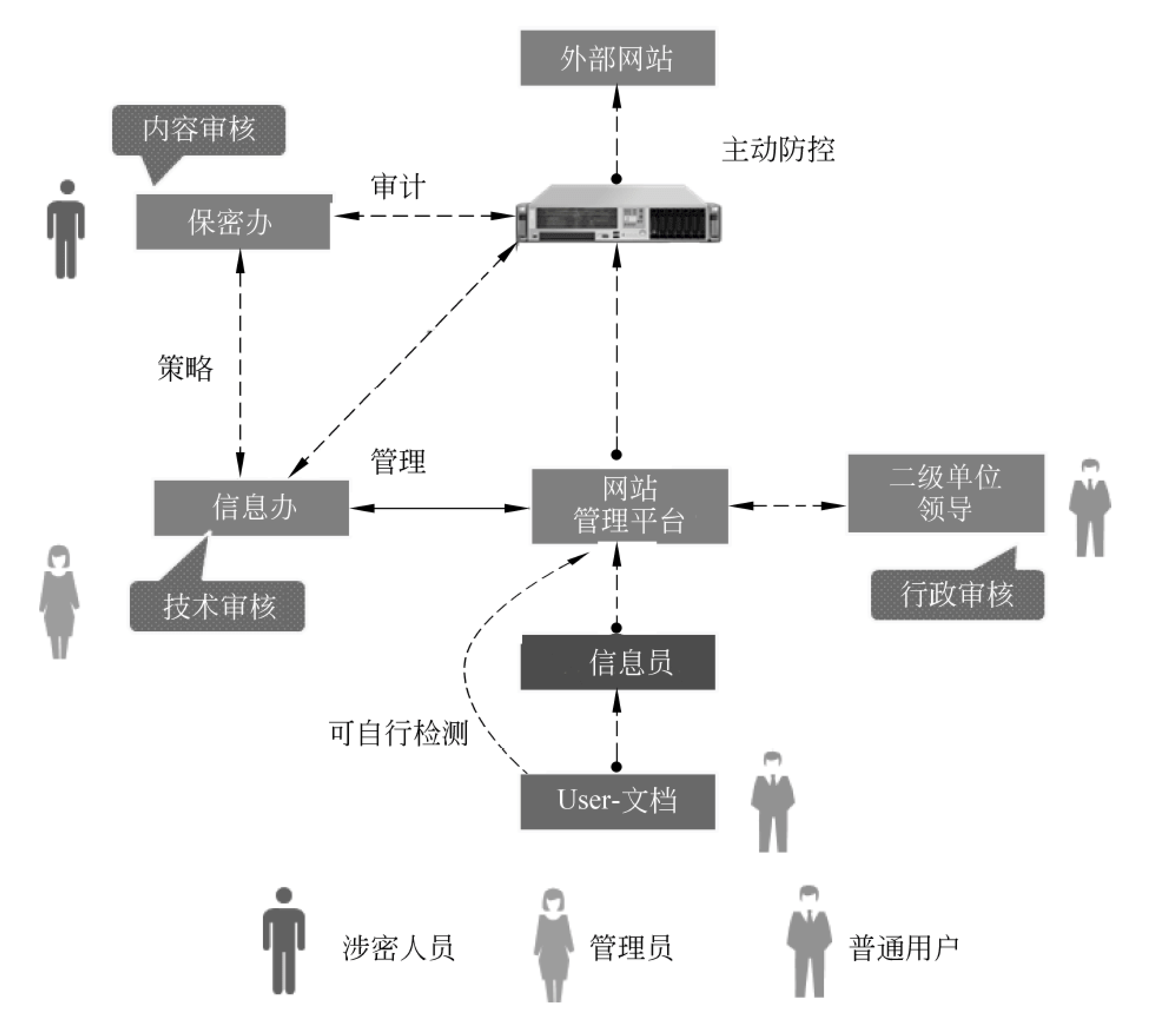


图 8-8　风险评估过程示意图

2. 文档发布涉密检查

高校为知识密集型组织，每年都会产生大量的学术论文，在这些论文通过各种渠道流入互联网之前，没有可界定文档是否涉密的技术手段，以人为判断为主。这样的审查机制不仅增加了审查人员的工作量，同时由于信息不对称（保密意识及保密知识的程度不同）的问题导致文档漏审，增加了泄密风险。文档涉密检查系统实现了用户在使用发布平台进行文件外发时，对外发的文件的自动涉密审查，降低了审查人员工作过程中漏审导致的泄密隐患。

文档发布涉密检查系统的典型架构如图 8-9 所示。

目前，高校普遍建立了信息门户。为方便使用，可以将文档涉密检查

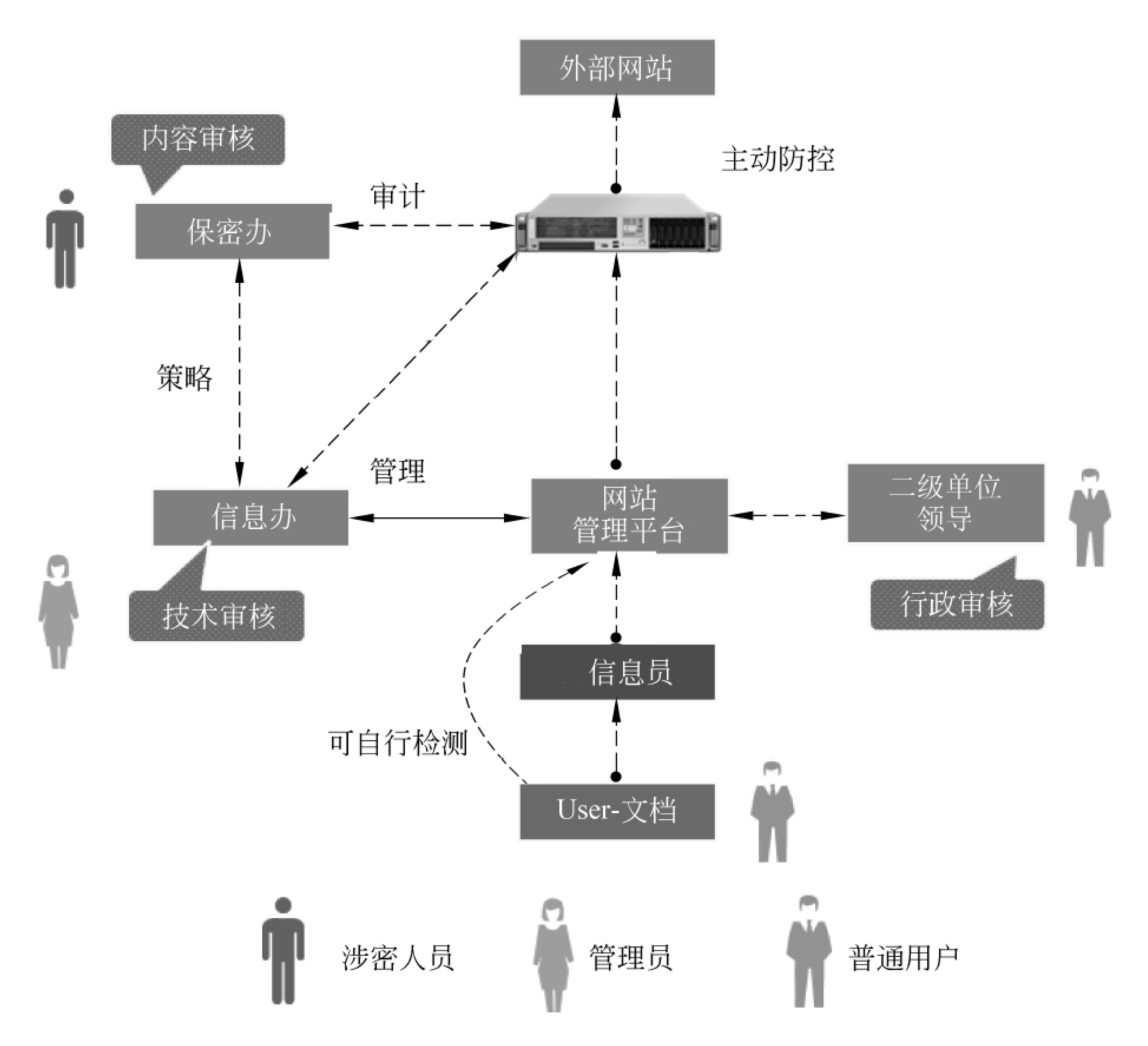


图 8-9　文档发布涉密检查系统

系统集成到门户中。普通用户登录门户网站保密专栏中点击检查链接自行检查，检查完成后形成检测报告；用户填写检测报告的审批表，交由二级单位领导进行内容审核；如果内容审核存疑则提交业务主管部门进一步审核；业务主管部门会根据检测报告和检测日志再次进行内容审核。只有审核通过后，用户才可进行文档信息的外发或外带。系统通过文档外发前的主动防控，可以有效防控文档泄密事件的发生。

3. 公共网络媒体保密监控

微博、微信、博客等公共网络媒体给高校计算机保密管理带来的主要威胁是有意或者无意地涉密信息泄露，可用于防范此威胁的保密管理技术是互联网信息内容审计技术。互联网信息内容审计系统根据用户提供的

网络链接(包括门户网站链接地址,微信、微博链接地址),利用网络爬虫技术对互联网数据内容进行分析筛选,对疑似涉密的内容进行分类分级,并将其中疑似度较高的内容提交人工审核和处理。

公共网络媒体保密监控的典型架构如图 8-10 所示。

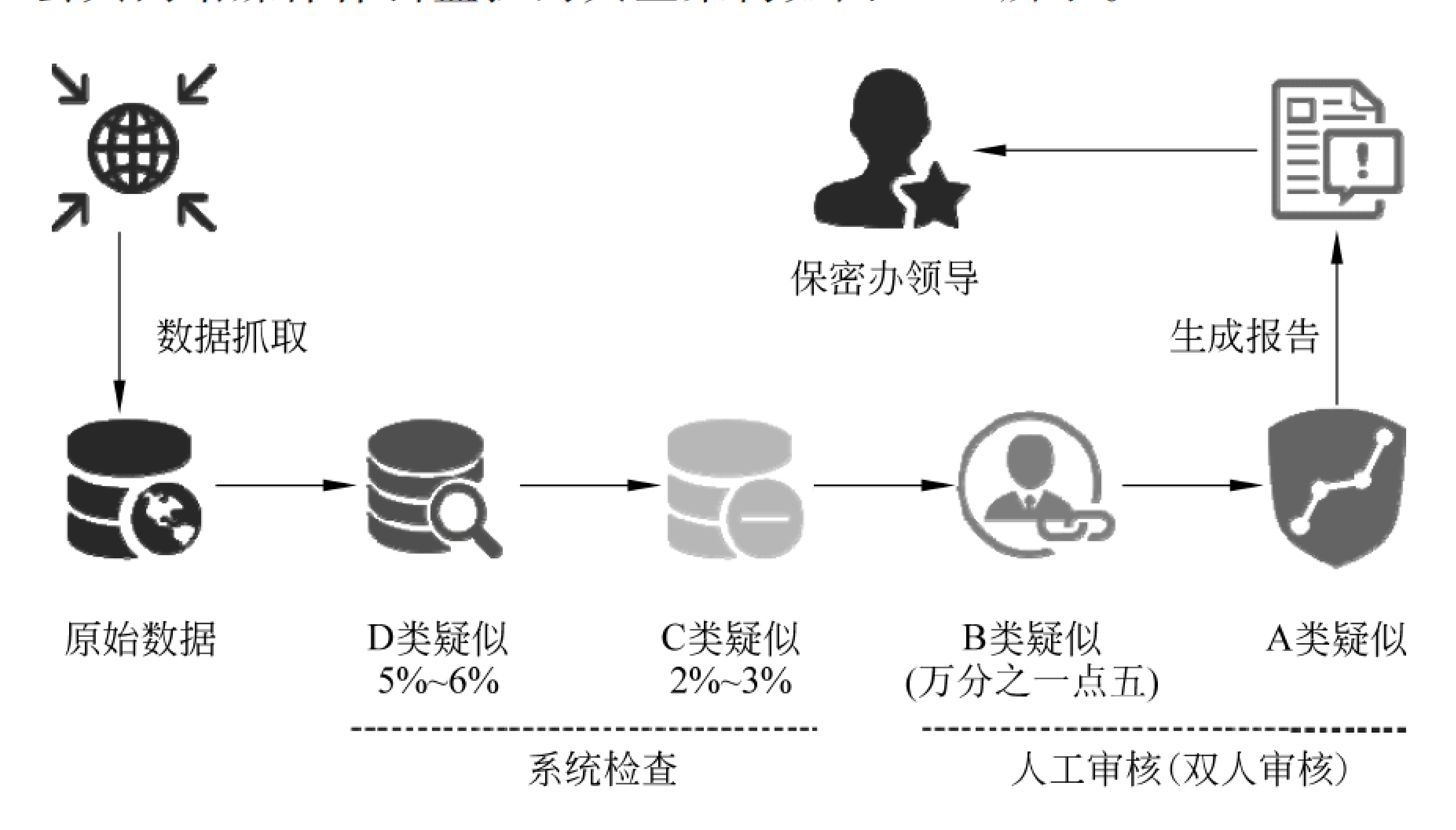


图 8-10 公共网络媒体保密监控

4. 非涉密计算机终端保密管理技术

高校非涉密计算机终端数量大、类型复杂、使用地点分散、管理难度高。针对非涉密终端的安全需求,目前可以提供如下安全技术手段:

(1) 安全配置技术。首先,制定互联网计算机安全配置技术和管理规范,自开发或者选购安全配置检测软件,对计算机选型及配置、操作系统安装及基本安全配置规范(系统服务、组策略配置、密码策略等)、常用软件白名单、日常使用、安全自查及常见安全问题处理等进行安全配置合规检测,帮助重点人员有效地配置和管理计算机,提高计算机更新及日常使用的效率。

(2) 安全检测技术。利用远程计算机漏洞扫描工具对重要计算机终端进行自动检测,并与定期检查(自查、院系检查及管理部门对重要人员的抽查等多种方式)相结合,形成对非涉密计算机终端有效的安全监控。

(3) 计算机终端安全审计技术。根据要求，应当对重要计算机终端进行网上审计。高校因为计算机终端的分散性，完全执行标准要求存在较大的实施难度。可以通过采用基于终端监控软件的计算机终端审计技术，从而实现针对重要计算机终端的日常行为、敏感信息等内容的审计，来满足相关标准的要求。

高校非涉密计算机位置分散，不宜集中管理。计算机终端监控与审计可以采用服务器、客户端的模式，其典型架构如图 8-11 所示。

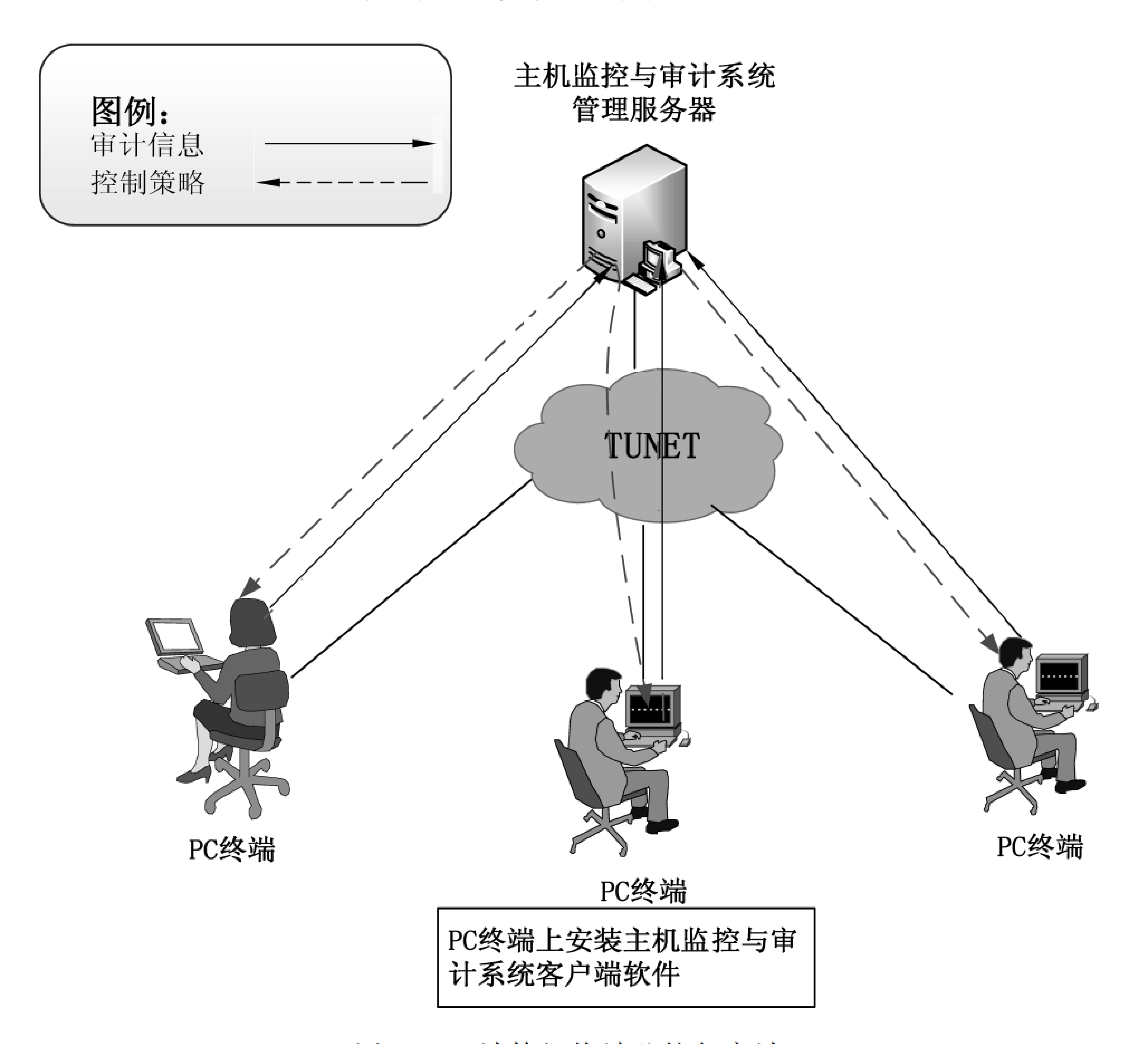


图 8-11　计算机终端监控与审计

在数据中心配置一台服务器安装监控服务器端，负责配置审计策略；需要监控的互联网计算机安装监控客户端；管理员在监控服务端配置监控

与审计策略，服务端将监控策略下发至监控终端，对其进行监控管理；监控客户端根据服务端下发的策略要求，将本地产生的重要报警、日志和审计信息上报到监控服务端；管理员可通过监控服务端查看审计日志与报警信息。

终端监控与审计网络访问行为审计和控制、主机重要操作的记录与审计、计算机内存储文件的涉密检查。网络访问行为包括：Web 浏览、电子邮件、网络文件传输等；可以通过黑白名单的方式对用户的网络访问行为进行控制；对用户上述范围内的网络访问行为进行记录和审计。

六、审计和风险自评估

为了及早发现和消除信息设备与存储设备失泄密隐患，应当定期进行审计和风险自评估。

（一）涉密信息设备和存储设备审计

涉密信息设备和存储设备审计由学校信息化管理部门负责，根据信息设备和存储设备的密级定期组织：秘密级计算机每 3 个月、机密级计算机每 1 个月、内部信息系统和信息设备每半年、互联网信息系统和信息设备每 3 个月审计一次。如果学校只有秘密级涉密计算机的，可以每 3 个月对互联网信息系统和信息设备及全部涉密计算机审计一次并生成审计报告，连续 6 个月的审计报告中还应当包含对内部信息系统和信息设备的审计；如果有机密级涉密计算机的，每个月应当对全部机密级涉密计算机审计一次并生成审计报告，连续 3 个月的审计报告中应当包含对互联网信息系统和信息设备及全部秘密级计算机的审计，连续 6 个月的审计报告中还应当包含对内部信息系统和信息设备的审计。

对信息设备和存储设备审计的流程通常为：

（1）由学校信息化管理部门负责制定涉密信息设备和存储设备的审计策略，包括审计范围、周期、内容等。

(2) 由学校信息化管理部门组织计算机安全保密管理员根据策略文件要求定期收集涉密信息设备和存储设备的审计日志,包括:违规外联日志、违规操作日志、文件操作日志、程序运行日志、上网行为日志、文件共享日志、文件打印日志、用户登录日志、网络访问日志、软件安装日志、违规使用日志、账户变更日志、刻录审计日志、文件流入流出日志、服务监控日志、主机状态日志等,形成审计报告的基本内容;对在审计中发现的问题和隐患,学校信息化管理部门应及时与保密管理部门沟通。

(3) 学校运行维护机构负责对计算机安全保密管理员形成的审计内容报告汇总,综合分析后形成审计报告,并对审计报告中提出的问题和隐患提出解决建议。

(4) 审计报告完成后由学校信息化管理部门负责人确认,并报学校主管信息化和主管保密工作的校领导审阅。

审计报告是基于涉密计算机导出的审计日志和自查的情况,结合对非涉密计算机和信息系统的安全审计情况,包含如下内容:

1. 整体运行情况

包括设备和用户的在线和离线、系统负载、网络和交换设备、电力保障、机房防护等是否正常。

2. 安全保密产品

对身份鉴别、病毒与恶意代码防护、主机监控审计、打印和刻录审计等安全保密产品的功能以及自身安全性进行审计。查验功能是否正常、日志是否完整,汇总日志发现是否存在违规行为。

3. 设备变更情况

对涉密计算机重新安装系统、硬件变更、权限控制等行为进行审计,防止故意隐藏或销毁违规记录,避免获取超出知悉范围的国家秘密。

4. 导入导出控制

对导入导出点的建立、管理和控制进行审计,对导入导出的审批流程、操作、行为和相关存储设备的使用等进行审计,特别是对以非密方式导出的信息进行审计。

5. 涉密移动存储设备

对涉密移动存储设备的授权、管理、存放、借用、使用、归还、消除和销毁等进行审计。

6. 涉密数据

对涉密数据的产生、修改、存储、交换、使用、输出、归档、消除和销毁等进行审计。

7. 用户操作行为

对用户使用涉密信息设备、涉密存储设备的关键操作行为进行审计。

8. 管理和运维人员操作行为

对管理员、运维人员等操作、维护安全保密产品的行为进行审计。

9. 内部信息系统和信息设备

对内部信息系统、内部信息设备和内部存储设备的配置、管理、使用、控制、安全机制等进行审计。

10. 互联网信息系统和信息设备

对互联网信息系统、信息设备和存储设备的配置、管理、使用、安全机制等进行审计。

根据审计过程中发现的信息设备和存储设备保密管理中的问题，以及审计报告中确定的整改措施和整改方案，由学校信息化管理部门组织学校运行维护机构和各相关涉密单位落实整改。

（二）风险自评估

信息化技术的广泛应用在提高科研、生产效率和质量的同时，也极大地增加了信息安全风险。目前解决信息安全问题普遍采用的方法是风险评估，从风险管理的角度，系统地分析信息系统所面临的威胁及其存在的脆弱性，评估安全事件一旦发生时可能造成的危害程度，并提出有针对性的防护对策和整改措施，将风险控制在可接受的水平，最大程度地保障信息安全。风险自评估是建立信息安全体系的基础和前提。涉密信息设备、

存储设备风险自评估报告根据单位的保密管理办法、信息安全保密策略，结合审计报告及日常使用情况，从物理安全、系统安全、信息安全、运行管理及应急安全四个方面进行风险综合评估，目的是查找脆弱性和威胁，确定风险和隐患，并及时采取整改措施。信息安全风险评估分为自评估和检查评估两种形式，可以由学校信息化管理部门在保密工作机构指导下进行，也可以委托国家保密行政管理部门设立或者授权的保密测评机构进行。这一部分将主要介绍学校自行组织风险自评估的工作开展的流程和基本步骤。

学校自行组织对涉密信息设备、存储设备的风险自评估的工作流程如下：

（1）由学校信息化管理部门牵头，组建由信息化管理部门、运行维护机构及相关管理部门组成的风险评估工作组，并制订风险评估工作计划。

（2）风险评估工作组根据风险评估工作计划开展工作，并根据评估结果形成风险自评估报告。报告形成后，由信息化管理部门报送学校保密工作委员会审批，并交保密管理部门存档。

（3）信息化管理部门根据风险评估中发现的问题制定整改方案，提供人、财、物等方面的支持，并监督运行维护机构落实整改措施。

风险评估的过程参见图 8-12，其分为背景建立、风险检测、风险评估和监督实施 4 个基本步骤。

1. 背景建立阶段

确定风险管理的对象和范围。风险评估不可能漫无目的地进行，应当首先明确范围，并对相关的信息进行调查分析，准备风险管理的实施。这一阶段由信息化管理部门牵头，明确范围和相关的评估人员。

2. 风险检测阶段

发现脆弱性和威胁，确定风险和隐患。这一阶段由评估人员按照明确的范围进行。

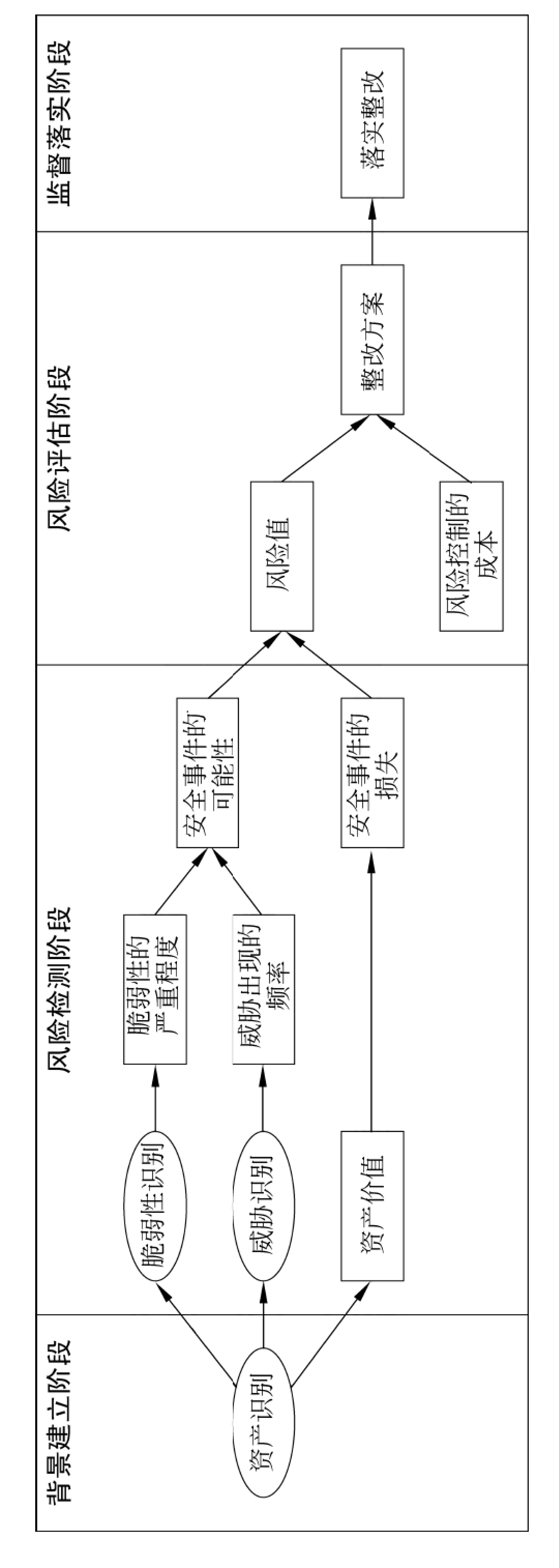


图 8-12　风险评估过程示意图

首先，要根据风险管理的范围识别资产。在表现形式上资产可分为数据、软件、硬件、服务、人员等类型。根据风险评估的范围识别出关键资产与一般资产，形成需要保护的资产清单。根据资产在保密性、完整性和可用性3个方面的安全属性，结合评估单位业务战略对资产的依赖程度等因素，对资产价值进行评估。

其次，分析资产所面临的威胁以及本身的脆弱性。威胁具有多种类型，如软硬件故障、物理环境影响、管理问题、恶意代码、网络攻击、物理攻击、泄密、篡改等。有多种因素会影响威胁发生的可能性，如攻击者的技术能力、威胁行为动机、资产吸引力、受惩罚风险等。在威胁识别阶段，评估者依据经验和相关统计数据对威胁进行识别，并判断其出现的频率。而脆弱性的识别可以以资产为核心，针对资产识别可能被威胁利用的弱点进行识别，也可以从物理、网络、系统、应用、制度等层次进行识别，然后与资产、威胁对应起来。脆弱性不会产生安全事件，只有威胁作用于脆弱性时才会导致安全事件的产生。

最后，从技术和管理两个层面，对信息系统所面临的风险并结合已采取的安全措施进行综合判断。确认安全措施是否有效抵御了威胁、降低了系统的脆弱性，并以此作为制订风险管理计划的依据和参考。

3. 风险评估阶段

通过对风险评估结果的等级化处理，综合考虑风险控制的成本和风险造成的影响，从技术、组织和管理层面分析安全需求，最终提出实际可行的安全措施。此外，还应当明确信息系统存在的残余风险以及可以采取的接受、降低、规避或转移等控制措施。这一阶段主要是由信息化管理部门组织不同层级的人员进行群体决策，可以利用咨询专家、构建风险分析矩阵或使用信息安全风险评估与控制类工具软件等多种方式进行辅助，最终形成对风险的分析和评估结果（报告）。

4. 监督落实阶段

其包括批准和持续监督两部分。风险评估报告应当报单位信息化管理负责人，依据风险评估的结果和处理措施能否满足要求，决定是否认可

风险管理活动及相应的措施。经批准后，由信息化管理部门组织并落实整改。除了对资产本身进行安全加固，整改还可以包括：通过规范策略、制度、操作规程实现 IT 服务和安全管理，保证业务的连续性；通过编写或修订安全保密策略、完善管理制度、规定详细具体的执行程序、明确责任部门和责任人等，将风险防控措施固化，以提供持续的信息安全保障；通过内部控制机制强化日常监督，结合保密检查、奖惩机制、绩效考核等手段，对风险控制措施进行强化落实等。

信息安全风险和安全需求会随着环境不断变化，信息安全风险评估是一个复杂、动态、循环的过程，通过动态的风险评估体系、动态的安全策略制定、动态的安全防护、实时的监控系统以及健全的安全管理体系，实现完整、动态的安全循环。

风险评估主要是为信息安全提供一个方向，不管采取的评估方法多详细、多专业，也只是描述信息安全风险状态，而不会改进评估单位的安全状态。只有切实利用风险评估结果强力推进改进活动，实现有效的风险管理，并保持其持续性，才能改善安全状态，进而保障系统安全。

附表 8-1　新增涉密信息设备和存储设备审批表示例

新增涉密信息设备和存储设备审批表

<table>
<tr><td>申请单位</td><td></td><td>责任人</td><td></td></tr>
<tr><td>设备分类</td><td colspan="3">计算机：□台　式(□中间机　□工作机　□输出机)
　　　　□便携式(□校内　　□校外)
外部设施设备：□打印机　□扫描仪　□读卡器　□其他________
存储介质：□优盘(□个人 □中转 □输出 □外携)
　　　　　□移动硬盘 □其他________
办公自动化设备：□复印机 □碎纸机 □其他________
声像设备：□照相机 □摄像机 □录音笔 □投影仪 □其他________
安全保密产品：□单向导入 □USB Key □其他______</td></tr>
<tr><td>设备品牌及型号</td><td></td><td>设备序列号
/硬盘序列号</td><td></td></tr>
<tr><td>涉密等级</td><td>□秘密　□机密　□绝密</td><td>固定资产编号</td><td></td></tr>
<tr><td>保密编号</td><td></td><td>放置地点</td><td></td></tr>
<tr><td>责任人涉密等级</td><td>□一般　□重要　□核心</td><td>责任人工作证号</td><td></td></tr>
<tr><td colspan="4">请在相应的“□”中打√
1. 严禁连接国际互联网，禁止与电话线相连　□已知晓
2. 设备须粘贴编号标识与警示标志　□已知晓
3. 若带有无线通信功能，须拆除相应模块或硬件　□已知晓　□不涉及
4. 涉密计算机须安装学校统一发放的操作系统和防护系统　□已知晓　□不涉及
5. 涉密计算机须专人专用，多人使用须采取相应安全策略　□已知晓　□不涉及
6. 曾经作为非涉密计算机使用的计算机须进行格式化　□已完成　□不涉及
本人已阅读并承诺严格遵守信息设备和存储设备保密管理办法及相关规定。
责任人签字：　年　月　日</td></tr>
<tr><td colspan="2">单位保密负责人意见：
符合实际工作需要，同意新增。
签字(公章)：　年　月　日</td><td colspan="2">定密责任人意见：
符合密级要求，同意新增。
签字：　年　月　日</td></tr>
<tr><td colspan="2">信息化管理部门意见：
同意新增。
负责人签字(公章)：　年　月　日</td><td colspan="2">运行维护单位：
已完成设备配置及台账填写。
操作人签字：　年　月　日</td></tr>
<tr><td colspan="4">维护过程记录：</td></tr>
<tr><td colspan="4">本人已领用该设备，从即日起对其安全保密负责。

责任人领用签字：　年　月　日</td></tr>
</table>

附表 8-2　涉密信息设备和存储设备变更审批表示例

涉密信息设备和存储设备变更审批表

<table>
<tr><td>申请单位</td><td colspan="2"></td><td>责任人</td><td></td></tr>
<tr><td>设备分类</td><td colspan="4">计算机：☐台　式（☐中间机　☐工作机　☐输出机）
☐便携式（☐校内　☐校外）
外部设施设备：☐打印机　☐扫描仪　☐读卡器　☐其他________
存储介质：☐优盘　☐移动硬盘　☐其他________
办公自动化设备：☐复印机　☐碎纸机　☐其他________
声像设备：☐照相机　☐摄像机　☐录音笔　☐投影仪　☐其他________
安全保密产品：☐单向导入　☐USB Key　☐其他______</td></tr>
<tr><td>保密编号</td><td></td><td>责任人涉密等级</td><td colspan="2">☐一般　☐重要　☐核心</td></tr>
<tr><td>申请变更事项</td><td colspan="4">☐涉密等级　☐放置地点　☐使用单位　☐责任人
☐使用情况（☐停用　☐启用）
☐重装操作系统　☐低级格式化
☐硬件安装、增减、拆卸（拆卸下的存储器件已按涉密载体管理
☐是/☐不涉及　接收人签字__________）
☐软件安装与卸载（注：白名单内的软件变更无须审批）
☐其他______________________</td></tr>
<tr><td>变更前</td><td colspan="4"></td></tr>
<tr><td>变更后</td><td colspan="4"></td></tr>
<tr><td colspan="5">变更理由及必要性说明：（可附具体变更内容清单。如申请变更责任人、使用单位，须由拟变更前后相关负责人或单位签字、盖章。）

责任人签字：　　　　　　　　　　　　　　年　　月　　日</td></tr>
<tr><td colspan="2">单位保密负责人意见：
符合实际工作需要，同意变更。
签字（公章）：　　　　年　　月　　日</td><td colspan="3">定密责任人意见：（密级/责任人变化时）
符合密级要求，同意变更。
签字：　　　　年　　月　　日</td></tr>
<tr><td colspan="2">信息化管理部门意见：
同意变更。请中心进行相关配置。
负责人签字（公章）：　　　　年　　月　　日</td><td colspan="3">运行维护单位：
完成设备配置及台账变更。
操作人签字：　　　　年　　月　　日</td></tr>
<tr><td colspan="5">维护过程记录：</td></tr>
<tr><td colspan="5">本人已领用该设备，即日起对其安全保密负责。

责任人领用签字：　　　　　　　　　　　　　　年　　月　　日</td></tr>
</table>

附表 8-3　涉密信息设备和存储设备报废审批表示例

涉密信息设备和存储设备报废审批表

<table>
<tr><td>申请单位</td><td colspan="2"></td><td>责任人</td><td colspan="2"></td></tr>
<tr><td>设备分类</td><td colspan="5">计算机：□台　式(□中间机　□工作机　□输出机)
□便携式(□校内　□校外)
外部设施设备：□打印机　□扫描仪　□读卡器　□其他________
存储介质：□优盘 □移动硬盘 □其他________
办公自动化设备：□复印机 □碎纸机 □其他________
声像设备：□照相机 □摄像机 □录音笔 □投影仪 □其他________
安全保密产品：□单向导入 □USB Key □其他______</td></tr>
<tr><td>设备涉密等级</td><td colspan="2">□绝密　□机密　□秘密</td><td>保密编号</td><td colspan="2"></td></tr>
<tr><td>固定资产编号</td><td colspan="2"></td><td>资产注销</td><td colspan="2">□是
□否</td></tr>
<tr><td>设备序列号
/硬盘序列号</td><td colspan="2"></td><td>整机报废</td><td colspan="2">□是
□否</td></tr>
<tr><td>报废原因</td><td colspan="5">
责任人签字：　　　　年　　月　　日</td></tr>
<tr><td colspan="2">单位计算机安全保密管理员意见：
经检查，上述信息属实。
签字：　　　　年　月　日</td><td colspan="4">单位保密负责人意见：
经审核，同意报废，申请销毁。
签字(公章)：　　　　年　月　日</td></tr>
<tr><td colspan="2">信息化管理部门意见：
同意。
负责人签字(公章)：　　　　年　月　日</td><td colspan="4">运行维护单位：
已接收，完成相关处理。
操作人签字：　　　　年　月　日</td></tr>
<tr><td colspan="6">处理记录：
拆除涉密存储硬件(固件)：□是(共______件，类型及序列号如下)　□否
____
____
____
安全技术处理：□是　□否
封存待集中销毁：□是(存放地点____________________)　□否
其他：

旁站陪同人签字：　　　　部件接收人签字：　　　　年　　月　　日</td></tr>
</table>

附表 8-4　涉密计算机信息导入审批表示例

涉密计算机信息导入审批表

<table>
<tr><td>申请单位</td><td colspan="2"></td><td>来源载体密级</td><td colspan="2">非密　□秘密　□机密</td></tr>
<tr><td>申请人</td><td colspan="2"></td><td>申请人涉密等级</td><td colspan="2">□一般　□重要　□核心</td></tr>
<tr><td>信息来源</td><td colspan="2"></td><td>来源载体类型
及编号</td><td colspan="2"></td></tr>
<tr><td>信息用途</td><td colspan="2"></td><td>信息去向</td><td colspan="2"></td></tr>
<tr><td>导入地点</td><td colspan="5"></td></tr>
<tr><td colspan="6">信息内容提要</td></tr>
<tr><td colspan="4">全文件名称</td><td>格　式</td><td>密　级</td></tr>
<tr><td colspan="4"></td><td></td><td></td></tr>
<tr><td colspan="4"></td><td></td><td></td></tr>
<tr><td colspan="4"></td><td></td><td></td></tr>
<tr><td colspan="4"></td><td></td><td></td></tr>
<tr><td colspan="2">项目负责人
意见</td><td colspan="4">□ 情况属实，同意申请。
签字：　年　月　日</td></tr>
<tr><td colspan="2">单位保密负责人
意见</td><td colspan="4">同意导入。
签字（公章）：　年　月　日</td></tr>
<tr><td colspan="2" rowspan="2">涉密中转优盘
借用与归还登记</td><td colspan="4">涉密中转专用 U 盘编号：______
借用签字：　年　月　日 ____ ：__ __</td></tr>
<tr><td colspan="4">本人已清空 U 盘。
归还签字：　年　月　日 ____ ：__ __
接收人签字：　年　月　日 ____ ：__ __</td></tr>
<tr><td colspan="2">操作人登记</td><td colspan="4">□ 已完成信息导入，导入内容与申请一致。
□ 中间机编号：______
□ 封闭光盘编号：______（非涉密中间机填写）
操作人签字：　年　月　日</td></tr>
<tr><td colspan="2">备　注</td><td colspan="4"></td></tr>
</table>

附表 8-5　涉密计算机信息导出审批表示例

涉密计算机信息导出审批表

申请单位		载体去向	
申请人		申请人涉密等级	□一般　□重要　□核心
输出原因			
输出地点			

制 作 明 细

制作方式	文件名称（可另附页）	密级	页数/文件数	份数/张数	受控编号
□打印 □刻录					
□打印 □刻录					
□打印 □刻录					

项目负责人意见	□同意　□不同意　输出。 签字：　年　月　日
单位保密负责人意见	□同意　□不同意　输出。 签字(公章)：　年　月　日
涉密输出优盘借用与归还登记	涉密输出专用 U 盘编号：＿＿＿＿ 借用签字：　年　月　日＿＿：＿＿
	本人已清空优盘。 归还签字：　年　月　日＿＿：＿＿ 接收人签字：　年　月　日＿＿：＿＿
操作人登记	□以上操作已完成，输出内容与申请一致。 操作人签字：　年　月　日
非密审查（导出内容为非密时须审查）	□ 经审查，输出的非密内容确实不涉及国家秘密，可以领用。 审查人签字：　年　月　日
领用登记	领用人签字：　年　月　日
备　注	

附表 8-6　携带涉密信息设备和存储设备外出审批表示例

携带涉密信息设备和存储设备外出审批表

<table>
<tr><td>申请单位</td><td></td><td>申请人</td><td></td><td>申请人
涉密等级</td><td>□ 一般
□ 重要
□ 核心</td></tr>
<tr><td>借用事由</td><td colspan="5">何地（　　　　　　　　）何事（□会议 □实验 □其他＿＿＿＿＿＿）
涉密工作或事项密级（□绝密　　□机密　　□秘密）</td></tr>
<tr><td>借用时间</td><td colspan="5">年　　月　　日　　至　　　　　　　年　　月　　日</td></tr>
<tr><td rowspan="6">拟外出携带
设备清单</td><td colspan="3">拟借用设备</td><td>涉密等级</td><td>数量</td></tr>
<tr><td colspan="3">计算机：□便携式（校外）</td><td>□秘密
□机密</td><td></td></tr>
<tr><td colspan="3">外部设施设备：□打印机　□其他＿＿</td><td>□秘密
□机密</td><td></td></tr>
<tr><td colspan="3">存储介质：□优盘　□移动硬盘
□其他＿＿＿＿＿</td><td>□秘密
□机密</td><td></td></tr>
<tr><td colspan="3">声像设备：□照相机 □摄像机 □录音笔
□投影仪 □其他＿＿＿＿＿</td><td>□秘密
□机密</td><td></td></tr>
<tr><td colspan="3">安全保密产品：□单向导入
□其他＿＿＿</td><td>□秘密
□机密</td><td></td></tr>
<tr><td>拟开放接口
和端口</td><td colspan="5">□打印　□刻录　□光驱读　□单向导入　□其他＿＿＿＿＿＿</td></tr>
<tr><td>设备携带
文件名称及
密级</td><td colspan="5"></td></tr>
<tr><td colspan="6">本人承诺遵守涉密信息设备和存储设备相关规定。设备中只存有与本次外出相关的涉密信息；使用后按期归还，并按要求对信息进行清除。因未采取保密措施，致使设备丢失、出现失泄密事件，本人承担相应保密责任。
申请人签字：　　　　　　　　　　　　　　　　　　　　年　　月　　日</td></tr>
<tr><td colspan="3">单位保密负责人意见：
符合实际工作需要，同意借用。
签字（公章）：　　　　　年　　月　　日</td><td colspan="3">信息化管理部门意见：
同意借用。
负责人签字（公章）：　　年　　月　　日</td></tr>
<tr><td colspan="6">运行维护单位：（如有操作，需附详细记录）</td></tr>
</table>

续表

<table>
<tr><td rowspan="6">借用
设备清单</td><td colspan="2">设备分类</td><td>涉密等级</td><td>保密编号</td></tr>
<tr><td colspan="2"></td><td>□秘密　□机密</td><td></td></tr>
<tr><td colspan="2"></td><td>□秘密　□机密</td><td></td></tr>
<tr><td colspan="2"></td><td>□秘密　□机密</td><td></td></tr>
<tr><td colspan="2"></td><td>□秘密　□机密</td><td></td></tr>
<tr><td colspan="2"></td><td>□秘密　□机密</td><td></td></tr>
<tr><td>开放接口和
端口</td><td colspan="4">□打印　□ 刻录　□光驱读　□单向导入　□其他 ____________</td></tr>
<tr><td rowspan="2">带出前</td><td colspan="4">□相关配置
□保密检查

操作人签字：　　　　　　　　　　年　　月　　日</td></tr>
<tr><td colspan="4">本人已领用上述设备，从即日起对其安全保密负责。
本人承诺按照学校有关规定，如实填写使用记录。

申请人领用签字：　　　　　　年　　月　　日 ______:______</td></tr>
<tr><td rowspan="6">使用记录</td><td>日期</td><td>时间</td><td colspan="2">操 作 事 项</td></tr>
<tr><td></td><td></td><td colspan="2"></td></tr>
<tr><td></td><td></td><td colspan="2"></td></tr>
<tr><td></td><td></td><td colspan="2"></td></tr>
<tr><td></td><td></td><td colspan="2"></td></tr>
<tr><td colspan="4">如实并详细记录开机、关机、输入、输出、外接等相关操作及内容。</td></tr>
<tr><td rowspan="2">归还后</td><td colspan="4">□相关配置
□操作审计
□保密检查
□信息消除

操作人签字：　　　　　　　　　　年　　月　　日</td></tr>
<tr><td colspan="4">本人如实填写使用记录，归还设备，并认可上述检查结果。

申请人归还签字：　　　　　　年　　月　　日 ______:______</td></tr>
</table>

第九章　科研活动和成果保密管理

要做好科研活动和科研成果保密管理，首先，需要全面识别涉密科研项目和涉密研究生学位论文工作中包含的科研活动以及产生的科研成果；其次，准确界定科研活动和科研成果是否涉密，进而依据规定采取针对性管理措施。

一、涉密科研项目过程管理

按照过程管理的思路，高校承担涉密科研项目一般可以分为项目论证、申报、立项、实施、结题验收等各个阶段。要做好涉密项目的保密管理，需要把保密要求融入项目管理和科研活动过程中，针对各个阶段的科研活动特点，针对性地实施保密措施，确保国家秘密安全。

（一）职责与分工

按照“业务工作谁主管，保密工作谁负责”的原则，项目负责人与各主要业务主管部门在涉密科研项目保密管理中职责与分工如下。

1. 项目负责人

项目负责人是涉密项目保密管理的第一责任人，直接负责组织落实所承担项目申报论证、立项、实施、验收和归档、鉴定报奖等全过程的保密管理工作。

2. 各承担涉密项目的院（系、所）

各承担涉密项目的院（系、所）是其所承担项目的保密管理责任主体，

对本单位涉密项目负直接管理责任,并为本单位开展涉密项目保密工作提供必要的组织保障和条件保障。

3. 科技处

科技处是学校涉密项目的业务归口管理部门,负责建立涉密项目动态数据库,组织开展与涉密项目相关的定密工作,完成与涉密项目相关的保密审查,协同保密管理办公室组织指导、监督检查相关院(系、所)在涉密项目全过程管理保密管理工作。

4. 档案馆

档案馆是学校档案工作的业务归口管理部门,负责学校涉密项目档案的接收、整理、保管和利用等工作。

5. 财务处

财务处是学校财务工作的业务归口管理部门,负责学校涉密项目经费预决算的审核、审计接待及经费的管理。

(二)论证与申报阶段的保密管理

科技处联合院(系、所)组织人员参与涉密国防科研规划建议与论证申报工作时,重点应当做好非涉密人员申报过程的保密管理工作(保密管理流程参见图 9-1)。

1. 做好人选把关

高校科研项目一般实行校级和院系两级管理和项目负责人负责制。高校人员成分复杂,应当在院系、研究所等的配合下,在组织人员查阅涉密项目申报指南时就做好人选把关,选择涉密人员以及具备涉密资格的非涉密人员进行申报。

2. 做好保密提醒

由于高校崇尚自由和创新的文化,相对缺少保密传统,科研人员思维发散,创新性强,崇尚自由,未承担过涉密项目、系统接受保密培训的师生,对保密工作的残酷性缺乏体验,往往保密意识淡薄,保密知识缺乏。因而,院系(所)在组织非涉密人员查阅涉密项目申报指南、接触涉密资料之前,

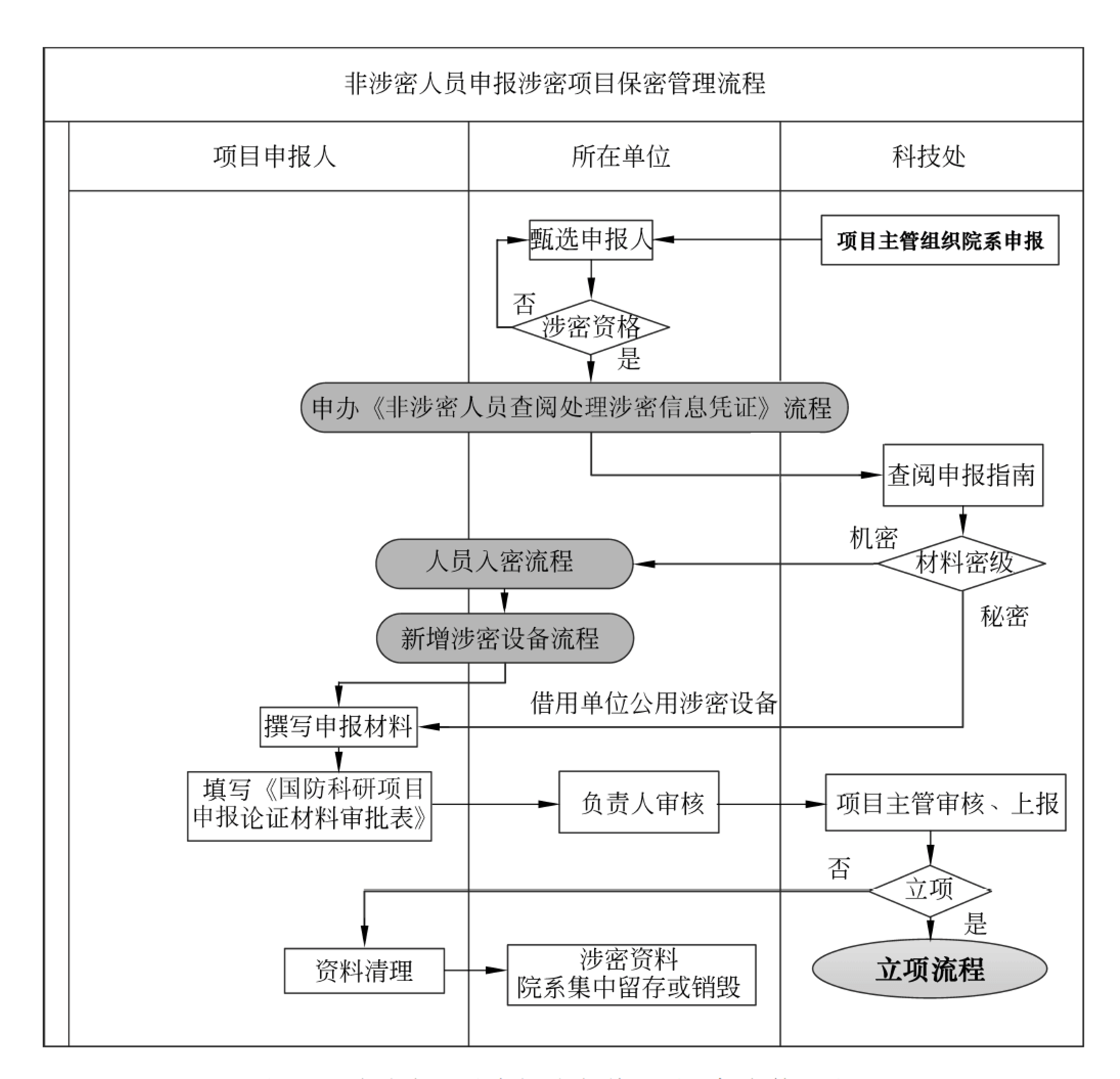


图 9-1　非涉密人员申报涉密科研项目保密管理流程

应当对其进行涉密资格审查,可以与人事处开展的涉密人员上岗前保密审查合二为一,不需重复进行;鉴于组织项目论证与申报工作时间较短,也可以根据实际情况适当简化资格审查流程(参见附表 9-1)。同时,还应当对其进行保密教育提醒,在其签署《查阅涉密信息保密承诺》(参见附件 9-2)后,方可查阅涉密资料。非涉密人员可以凭《查阅处理涉密信息保密承诺》或院系专门发放的“查阅处理涉密信息凭证”(参见附件 9-3)查阅项目申报指南、接触涉密文件,使用秘密级公用涉密设备处理,非密人员申办查阅处

理涉密信息凭证简化流程参见图 9-2。

《非涉密人员查阅处理涉密信息凭证》申请流程
非密项目提议人
所在单位
科技处
填写《人员资格审查表》
负责人审核
保密提醒
签署保密承诺书
领取《非涉密人员查阅处理涉密信息凭证》
查阅涉密信息
借用秘密级公用涉密设备

图 9-2　非密人员申办查阅处理涉密信息凭证简化流程

3. 做好保密条件保障

为了避免从源头出现泄密和违规事件，进行涉密科研项目申报时的材料，均应当按照拟定密级进行管理。对于非涉密申报人员，因尚不具备涉密计算机等基本硬件条件，院系（所）或学校应当为其提供涉密计算机及打印机等条件保障，在计算机保密管理员的监督指导下使用。

鉴于非涉密人员不得使用机密级（含）以上涉密设备，如果按照申报要求需要提交机密级（含）以上涉密资料，则需要履行入密手续，正式纳入学校涉密人员管理，配备相应密级的涉密设备。

4. 做好申报材料清理

如非涉密人员申报的涉密科研项目未立项，需及时删除销毁相关论证与申报材料，或交由院系集中保存，个人不得保留标密文件。

（三）立项阶段的保密管理

对于获准立项的涉密项目，应当事先确定涉密事项，确认具备开展保密工作条件后，方可办理合同签订手续（管理流程参见图 9-3）。

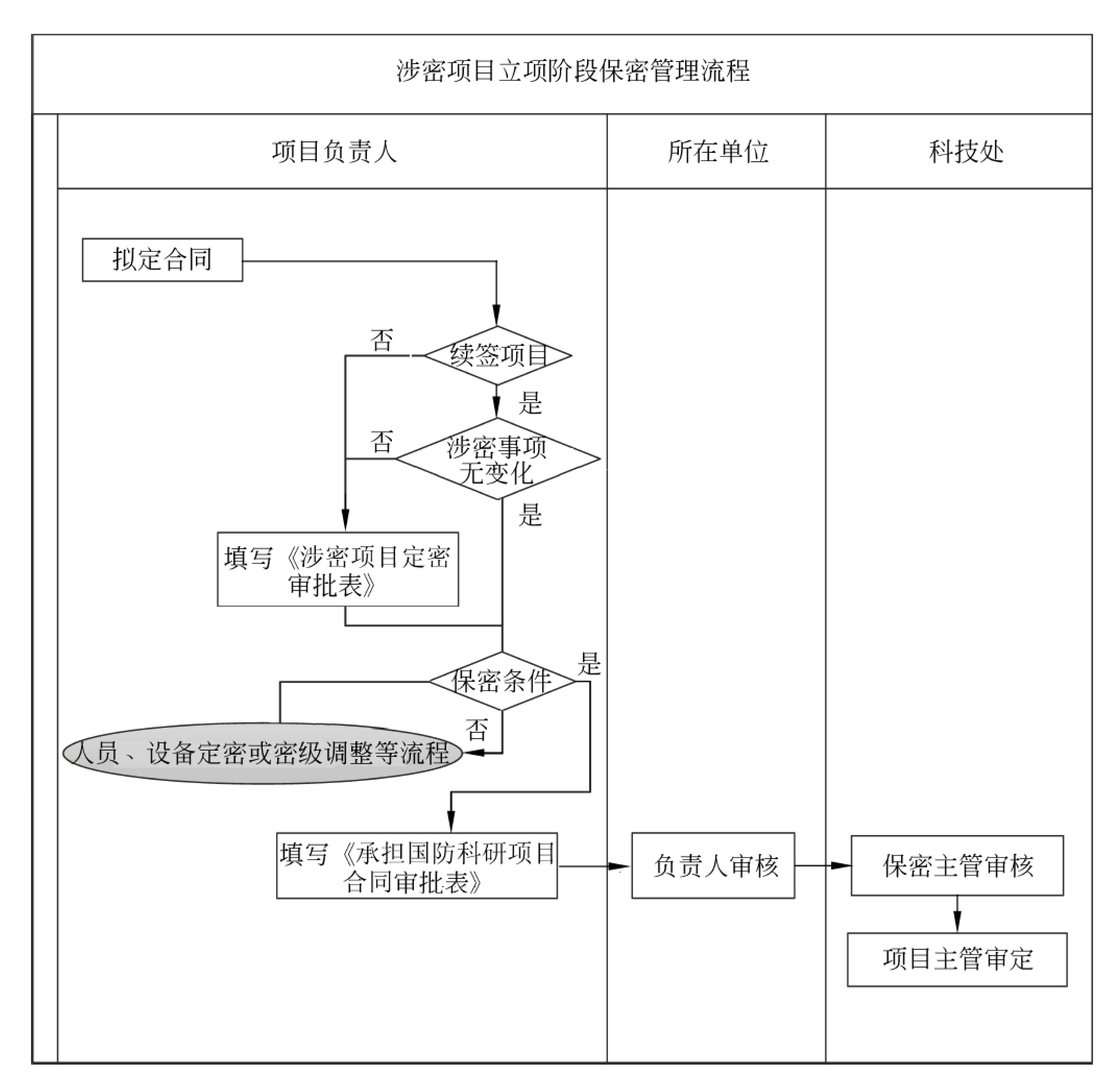


图 9-3 立项阶段保密管理流程

1. 做好项目定密

高校涉密领域点多面宽，准确定密较为困难。而对每一项涉密事项进行保密管理，都离不开掌握涉密信息的人员、涉密信息的载体、处理涉密信

息的设备、存放涉密信息的场所等要素。因而，在高校涉密科研保密管理中应当以涉密事项确定为源头，做好保密体系人、机、载体、场所的定密管理。

涉密科研项目获准立项后，项目负责人应当选择具备涉密资格的人员组建涉密课题研究队伍，并依据项目合同书、任务书、保密协议书等甲方约定或保密事项范围的规定，本着“具体化、精准化”的原则，明确该项目的涉密事项（如项目来源、军事需求、项目应用背景、核心技术、关键技术指标等），按照尽量缩小知悉范围的原则，合理分配研究任务，设置涉密岗位，明确各涉密事项的知悉范围（参见第四章附表 4-3），知悉范围内的人员均需纳入涉密人员管理范围。同时，为了降低涉密人员的流动性，尽量减少研究生涉密，并尽可能选择来源于国防单位（如为强军计划培养的研究生）或有志于服务国防部门的政治可靠的研究生进入涉密岗位。

2. 做好保密条件审查

为了解决涉密项目立项后部分院系保密条件建设滞后的问题，高校应当在签订合同前对是否具备保密条件进行审查。项目负责人及所属院系应当对照项目包含的各涉密事项的密级和知悉范围，核查项目组是否具备开展保密工作的条件。开展保密工作条件包括：参与涉密工作人员的涉密等级、所用的涉密设备与开展涉密工作的场所是否符合保密要求等。需要新增涉密人员或变更涉密人员涉密等级的，或需要增加涉密设备或变更涉密设备密级的，或需要对开展涉密工作场所增加防护设施的情况，都属于尚不具备保密条件的情况，院系应当认真核查，确保课题组具备开展保密工作的条件后才履行合同签订手续。

鉴于高校各承担涉密科研项目院系的保密管理水平参差不齐，为了加强合同签订前的保密条件审核把关，可以采取单独设计保密条件审查表的方式，由保密管理办公室组织对人员、设备、场所等相应条件进行审核确认；或由保密管理办公室协调信息办、人事处、保卫处等相关业务归口管理部门在项目立项前对拟承担涉密课题研究的课题组相应条件进行现场检查确认；也可以采用书面审查与现场检查相结合的方式，比如从事涉密科

研工作三年以上的项目负责人,新增项目立项前对其保密条件的审查采取书面审查方式;不足三年的,对其课题组进行现场检查。

(四)项目实施阶段的保密管理

在涉密科研项目的实施阶段,项目组应当严格执行学校各项保密管理制度。项目组专兼职保密员协助项目负责人收集、保管项目资料,落实本项目组的涉密人员、涉密载体、计算机、涉密场所以及有关涉密活动的日常保密管理工作。学校保密管理办公室与相关业务归口管理部门需要重点做好以下工作。

1. 做好保密培训

高校涉密项目以基础研究、预先研究为主,项目数量多、规模小、周期短,客观上导致涉密人员数量多、流动性强。持续强化有关人员保密意识、不断提高防范能力是做好高校保密工作的根本。应当将涉密程度深,承担涉密项目多、涉密时间长的重点人员作为保密提醒与保密检查的重点,其他涉密人员也应当参加学校定期组织的保密培训和考核。

2. 做好动态管理

伴随科研项目的开展,项目负责人需要及时对任务分工进行调整,对涉密人员、计算机、存储介质以及涉密场所等要素进行动态管理。人员管理方面,对拟新进入或脱离涉密岗位的人员按照涉密人员管理的有关规定履行相应入密或脱密手续;设备管理方面,对新增或需要报废涉密计算机与办公自动化设备及时履行审批手续,并做相应的技术处理。项目负责人因故需要变更,或项目因故需要转出学校时,除了按照项目管理要求履行相应变更手续外,应当同时履行定密、涉密人员及信息设备等有关变更手续,做到对各个院系(所)承担的涉密项目清楚,对各个涉密项目包含的涉密事项、涉密岗位、涉密人员清楚,对各个涉密人员使用的涉密计算机、涉密存储介质清楚。

3. 做好关键活动审查

高校具有环境开放,科研场所分散,师生与社会的各方联系紧密,国内

外的交流频繁,发表学术论文、出版学术专著普遍,网络四通八达、对外信息发布多等特点,增加了失泄密的风险,加大了保密管理的难度。因此,切实加强保密审查,做好涉密部门、部位来访接待、对外交流、发表论文、信息发布等关键环节以及涉密会议、外场试验与外协等关键活动进行保密提醒与审查非常重要。为了保证审查的有效性,提高审查效率,应当充分借助院系保密工作领导小组的力量。

4. 做好保密检查

高校信息化程度高,通信网络四通八达。信息安全管理始终是高校最大的泄密隐患。教师个人往往拥有多台计算机和存储介质,非涉密、涉密信息交换频繁,泄密风险大。针对这一现状,一方面,高校应当大力加强计算机的技术防范能力,从技术上降低泄密的风险;另一方面,应当加大保密检查力度,强化监管职能。通过院系自查和学校抽查相结合,定期检查、专项检查和不定期抽查相结合等检查方式,并使用专用计算机保密检查工具,不断加大保密检查的深度,进一步提高涉密人员的保密意识与防范能力,加深对保密管理制度的理解与掌握。同时,对检查中发现的问题,限期整改,根据奖惩规定,严肃处理,确保制度的执行力,有利于及时消除失泄密隐患,有效避免失泄密事件的发生。

5. 做好其他环节审查

高校诸多教师在承担军口科研项目的同时,也承担了大量民口科研项目和教学任务,身份交织,需要在涉密工作与非涉密工作之间不断转换角色,容易造成涉密界限不清。伴随高校涉密科研项目的开展,还涉及财务管理、设备购置管理、涉密人员申报非涉密项目以及职称评定等多种活动。这些活动一旦处理不当,很可能暴露项目来源、研究内容、甚至关键指标等涉密或敏感内容。比如在财务管理过程中,录入涉密项目到款信息、项目财务账户命名及报销过程、经费决算及审计过程以及申请免税环节,均可能涉及项目来源等信息;在设备购置管理中,设备购置申请以及申报免税过程需填报设备用途、经费来源等信息;在涉密人员申报非涉密项目以及职称评定时,为了充分体现申请者的工作基础或水平,申报材料内可能包

含对已承担涉密课题的阐述。在这些活动过程中,应当以“尽量缩小知密范围”为原则,尽可能对相关信息做非密化处理,院系(所)进行保密审核,确保材料不涉密后方可报出;对于必须涉密的环节,如涉密项目财务决算等过程,则需选择使用符合保密要求的设备和环境以及传输方式进行处理。

(五)结题验收阶段的保密管理

在涉密项目的结题验收阶段,项目组除了按照任务下达部门完成有关材料准备、会议答辩外,还需要做好资料归档及与项目相关人员、设备、资料的清理工作(管理流程参见图 9-4)。

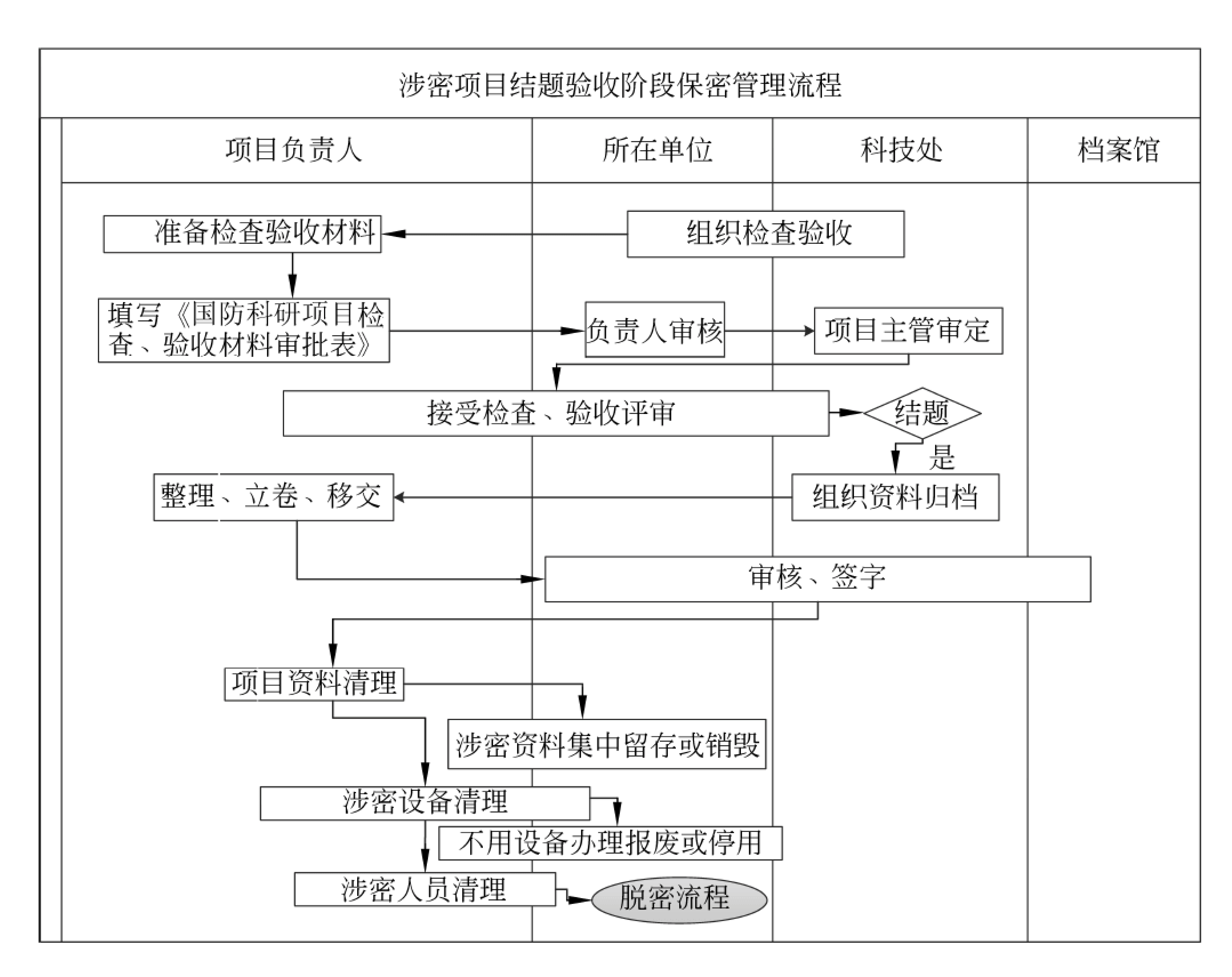


图 9-4　结题验收阶段保密管理流程

1. 做好资料归档

项目结题后，学校科研管理部门联合相关院系（所）组织项目负责人及课题组，按照学校国防科研项目立卷归档的有关规定，向档案馆提交归档资料。为了确保资料归档及时完整，应当在立项之初，对有归档要求的项目组明确提出归档范围，并在验收阶段，再次提出归档时限要求。项目组兼职保密员应当在科研过程中注意拟归档资料的收集整理，并按档案管理的有关规定及时归档，归档过程中文件传递及保存应严格遵守涉密载体管理的有关规定。

2. 做好资料、设备、人员清理

项目结题后，项目组专兼职保密员应当督查项目组成员清理与涉密项目相关的资料（包括纸质载体和电子文档），无须保留的及时交由院（系、所）销毁，需要保留的由院（系、所）或具备保存条件的项目组集中保管；不再使用的涉密设备，及时办理停用或报废手续；对未承担其他涉密岗位且未申请新涉密项目的人员，在对其负责或参与的所有涉密项目结题确认后（参见附表 9-4），按规定应当及时办理脱密手续，并要求其逐项清理（退）各类涉密载体，由项目负责人（导师）或者系保密工作负责人对清理（退）情况进行把关。

二、协作配套管理

根据科研工作需要，高校承担的部分涉密科研项目需要通过校外协作或校内分包来完成。对校外协作的涉密项目，重点做好合同签订前的保密审查与合同执行期间的保密监督检查；对校内分包的涉密项目，关键做好合同签订前的密级分解，合同执行过程具体遵照学校涉密项目保密管理规定执行。

（一）职责与分工

涉密科研项目负责人负责选择协作配套单位，分解外协/分包任务密级与涉密事项。学校科技处负责外协/分包任务在立项阶段的保密审查，

并协同或配合学校保密管理办公室，对外协/分包项目执行过程中的保密管理进行指导、监督和检查；保密管理办公室负责组织开展外协任务执行过程中的保密监督检查。

（二）校外协作保密管理

外协涉密项目保密管理流程参见图 9-5，主要包括：

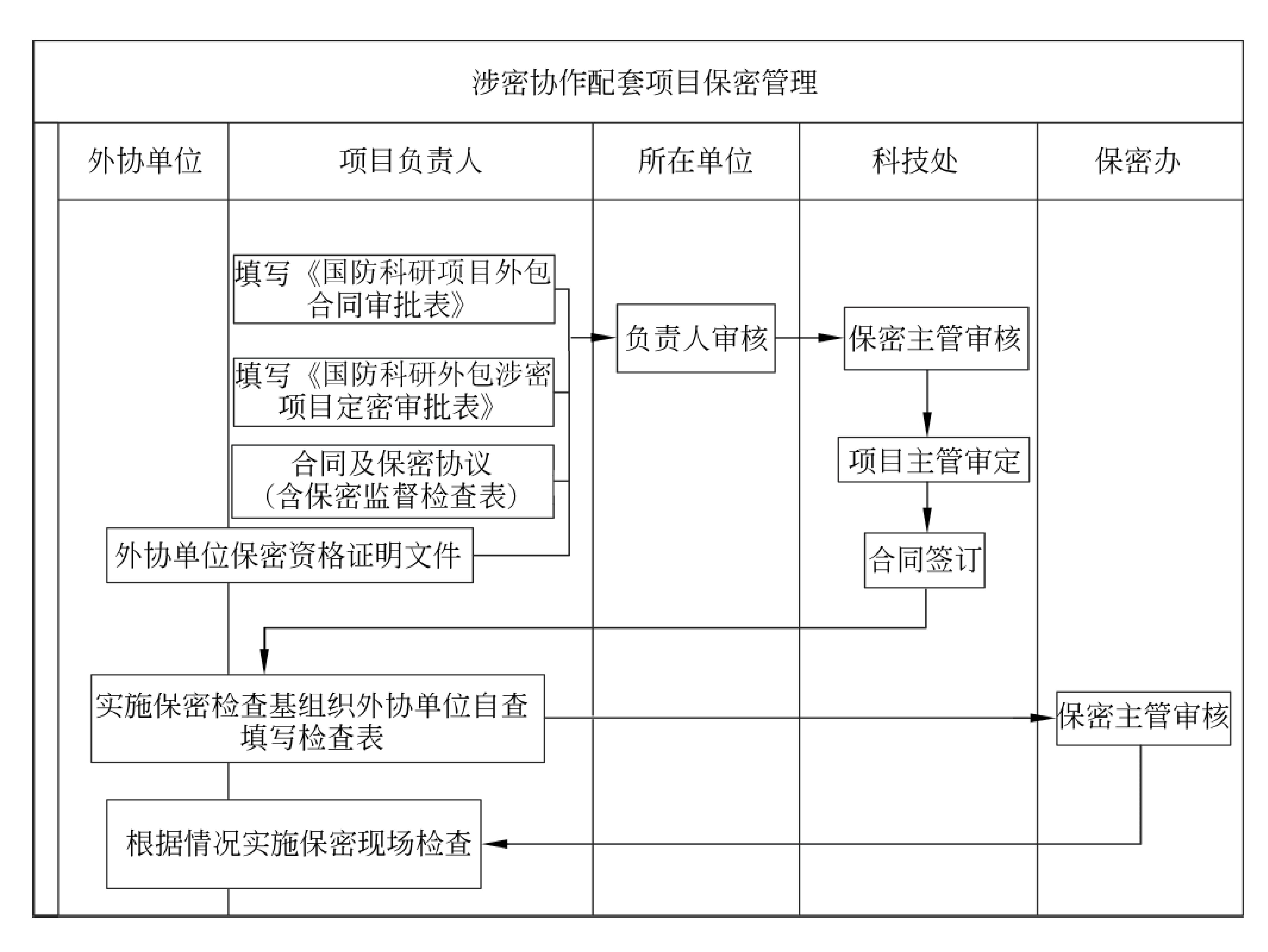


图 9-5　校外协作涉密项目保密管理流程

1. 立项前保密管理

在合同谈判以及合同文本中，项目负责人应当本着尽量缩小涉密事项知悉范围的原则，严格控制背景、用途等涉密内容，不得泄露和提供配套项目研制必需的技术要求以外的涉密信息。

外协任务必须涉及项目涉密事项的，则按照其所包含涉密事项中最高密级及最长保密期限要求，提出外协任务的建议密级与保密期限，并按以

下原则选择具有相应保密资格的协作配套单位：①外协项目为绝密级的，协作配套单位应当具有一级保密资格；②外协项目为机密级的，协作配套单位应当具有二级及以上保密资格；③外协项目为秘密级的，协作配套单位应当具有三级及以上保密资格。

2. 立项阶段保密审查

在外包项目合同文本中，应当明确项目密级；项目涉密的，还应包含保密条款，明确涉密事项与保密期限，并签署保密协议，选择的协作配套单位还需提供保密资格证书等证明材料。

由科技处对外协任务的项目密级、期限、协作配套单位保密资格、合同保密条款及保密协议等进行审核，通过后方能签订外协合同。

3. 执行阶段保密管理

在外包涉密项目合同履行过程中，项目负责人应当严格控制涉密事项知悉范围，不得泄露和提供超出配套项目研制所必需的涉密信息，并经常对协作配套方进行保密提醒，要求其严格执行合同中的保密条款，遵守保密协议。

在合同履行中，如协作配套单位的保密资格发生变更，项目负责人应当及时将变更书面证明材料提交学校科技处备案。

4. 保密监督检查

为了有效监督涉密协作配套单位对合同保密条款及保密协议的执行情况，在涉密外包项目合同履行期间，项目负责人应当对其涉密协作配套单位的保密管理情况进行至少一次监督检查，学校保密管理办公室可根据需要对重点协作配套单位组织现场检查。

保密监督检查可采取现场检查或函调等方式，实施检查者或接受检查单位都需要填写“涉密协作配套单位保密监督检查表”（参见附表 9-5）。针对检查发现的问题，应当向协作配套单位提出整改意见，并对其整改情况进行跟踪检查。对保密责任不落实、整改不到位的协作配套单位，视其影响程度，科技处暂停拨款或扣除部分合同经费，必要时中止合同，并追究其违约责任。

（三）校内协作保密管理

由校内二级单位分包的涉密的项目，其密级不应高于母项目的密级。由委托方与承担方的项目负责人及所在院（系、所）明确涉密事项，由承担方确认具备开展保密工作条件后，到科技处接受定密审查和履行合同审批手续（流程参见图 9-6），之后按照涉密项目过程管理的有关要求执行、实施。

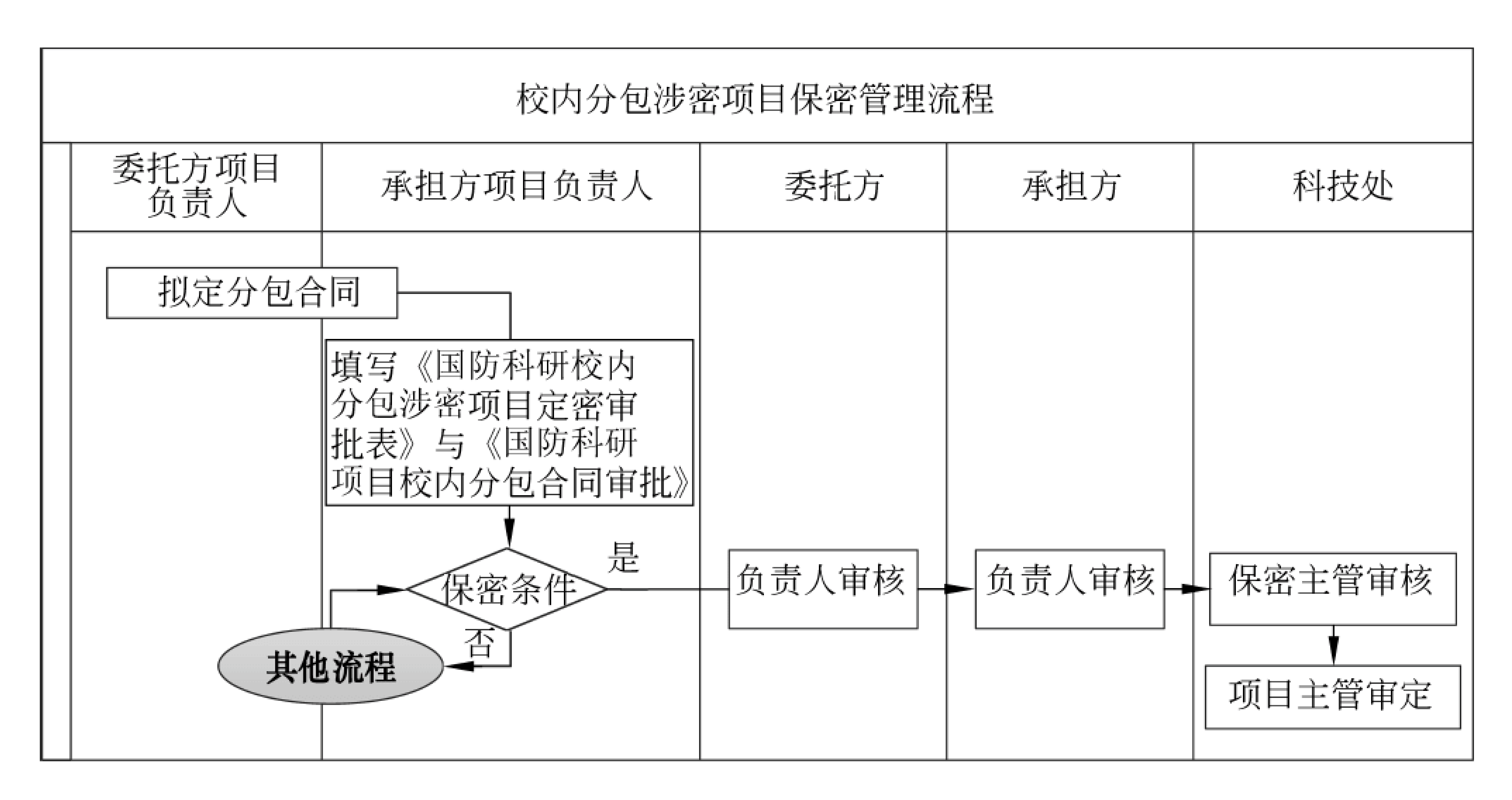


图 9-6　校内分包涉密项目立项管理流程

三、研究生学位论文工作的保密管理

为了做好研究生学位论文工作的保密管理，应当将保密要求融入学位论文研究和管理工作中，按照规定做好学位论文开题、中期考核、学术报告、论文评阅、答辩、学位审议、存档保管、查阅利用等各个环节的保密管理工作。

（一）职责与分工

研究生指导教师（以下简称“导师”）是研究生学位论文工作的保密负责人；有关定密责任人负责做好学位论文定密工作；研究生院是研究生学

位论文保密管理的归口管理部门，应当把研究生学位论文工作的保密管理要求融入研究生培养的各个环节中，并组织实施；各院系负责组织落实研究生学位论文日常保密管理工作；档案馆负责归档后学位论文的保管与利用工作；图书馆负责公开后的学位论文保管和利用工作；保密管理办公室负责对研究生学位论文工作保密管理的指导、监督和检查。

（二）论文开题前的保密管理

研究生学位论文开题是研究生学位论文工作正式启动的标志，与涉密项目立项前的保密管理类似，需要完成对学位论文的定密工作，同时确保研究生的涉密等级符合涉密学位论文工作要求。

1. 学位论文定密申请

学位论文内容涉及国家秘密的，导师和研究生应当在开题前向培养单位的研究生教务部门提出学位论文定密申请，经研究生教务部门对研究生涉密身份及开题时间等信息进行审核确认后，按照程序报培养单位定密责任人或有相应定密权的上级机关、单位审定（参见附表 9-6），审核结果报培养单位研究生教务部门备案。流程参见图 9-7。

2. 定密审核要点

来源于校内涉密项目的学位论文的密级不得高于项目密级，涉密论文的保密期限不得超过项目保密期限，同时，研究生作为项目参与人员应当在涉密项目所确定的涉密事项的知悉范围之内。

涉密学位论文来源于校外课题时，论文作者需要同时提供校外单位开具的定密证明。

无涉密项目背景、但论文内容涉及国家秘密事项的，申请论文涉密时须在“申请论文保密的理由”栏对照国家保密局分别会同中央、国务院有关部委制定的《国家秘密及其密级具体范围的规定》具体写明定密依据。

3. 涉密研究生管理

导师应当在论文开题前将参加校内涉密项目研究的研究生按涉密人员管理相关程序及时将其纳入涉密人员进行管理，涉密等级应当满足涉密

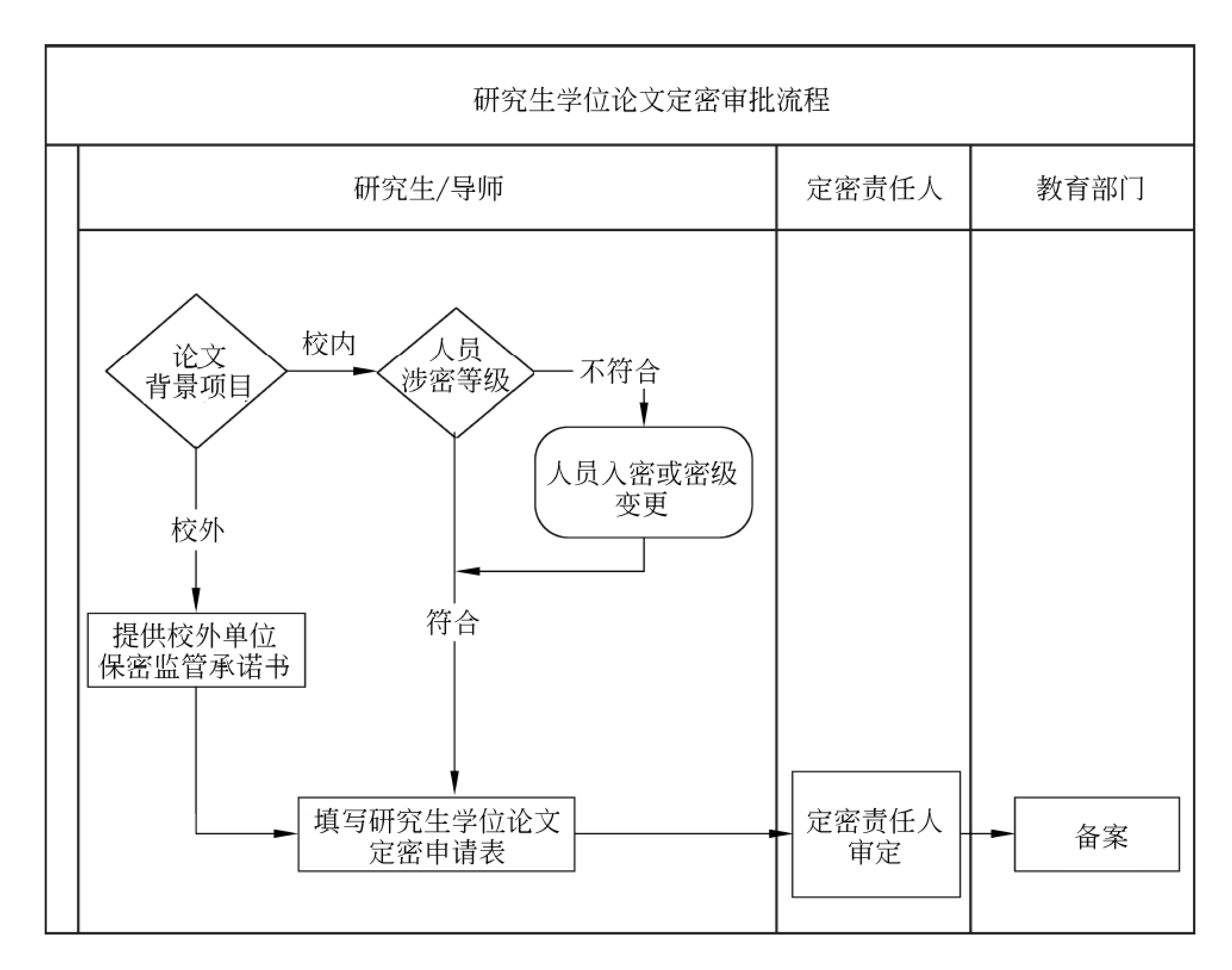


图 9-7　研究生学位论文定密审批流程

论文工作的要求，并为其提供开展符合保密要求的信息设备与涉密场所等保密工作条件；参加校外单位的涉密研究工作的研究生，原则上应当由校外单位提供保密工作条件并接受校外单位的保密管理，需要提供“校外单位保密监管承诺书”（参见附表 9-7）报所在院系保密工作领导小组备案。

（三）论文形成阶段的保密管理

学位论文形成阶段是学术成果产生的关键阶段。研究生应当严格遵守学校的各项保密管理制度，重点做好涉密论文形成及研究生培养各环节中涉密活动的保密管理。

1. 涉密学位论文撰写与制作

涉密学位论文应当视为国家秘密载体进行严格管理，在封面或首页做出国家秘密标识，涉密内容的撰写及修改必须在涉密计算机上进行，传递、

打印、复制等过程也需要符合相关保密要求。

为了保证研究生培养环节各项工作和学位审批工作的正常开展，涉密学位论文的题目和摘要内容一般不得涉密。

2. 相关涉密活动

涉密学位论文的研究过程涉及开题报告、中期考核、最终学术报告等环节这些环节如果涉密，相关的涉密材料应当按照学校涉密载体的规定进行管理，相关会议的组织也应当符合学校涉密会议的相关规定。

3. 涉密论文定密变更

涉密学位论文密级或保密期限在学位论文工作过程中确需调整时，导师应当依照学校有关规定及时履行变更手续。

（四）论文答辩阶段的保密管理

学位论文答辩阶段的保密管理重点是按照学校涉密载体与涉密会议等管理规定，做好论文的评阅、答辩、学位审议、学位论文提交等环节的保密管理。

1. 涉密学位论文评阅、答辩及审议

为了不扩大涉密学位论文的知悉范围，研究生院一般不对涉密学位论文进行隐名送审，而由导师在论文知悉范围内拟定评审专家名单，培养单位通过机要交通、机要通信或者专人递送等方式送达评阅人及收回论文与评审意见。为了明确保密责任，涉密学位论文的评阅人、答辩专家以及相关学位审议人员等接触论文涉密内容的人员还应当签订保密协议书。论文答辩以及学位审议等环节涉密的，需要按照涉密会议有关规定执行。

2. 涉密学位论文提交

学校学位评定委员会对研究生做出授予学位的决定后，有关的纸质涉密学位论文和电子版本应当按照学校管理要求，由研究生本人或教务部门将学位论文依据涉密载体传递有关规定和流程，送交学校档案馆保存，研究生本人不得私自留存涉密学位论文。

3. 学位（毕业）审批材料的保密管理

为了控制学位论文涉密事项的知悉范围，学位（毕业）审批材料（正本）

原则上不得涉密，必须涉密的应当按照定密管理有关规定在涉密的学位(毕业)审批材料封面的左上角做出国家秘密标识，并按照学校涉密载体相关规定进行管理。同时，按照研究生培养要求，存入研究生人事档案的学位(毕业)审批材料(副本)不得涉密。

4. 毕业研究生的保密管理

涉密研究生毕业离校前，应当按照学校涉密人员管理相关规定履行脱密手续，所在院系或学校保密管理办公室对其进行保密教育谈话。脱密期内培养单位应当掌握其就业、去向等相关情况。

(五) 论文归档后的保密管理

涉密学位论文归档后除由档案馆按涉密载体妥善保管外，重点依据涉密载体与定密管理有关规定做好学位论文利用过程的保密管理，以及定密变更、解密等工作。

1. 涉密学位论文利用

涉密学位论文在保密期内，不得以任何方式对外公开，有关人员经导师或培养单位保密主管领导批准后方可查阅。

2. 涉密学位论文定密变更

需要变更密级或保密期限的涉密学位论文，导师须提交学位论文定密变更申请表；源于校外涉密项目的研究生学位论文，应当由项目来源单位提供论文定密变更的书面通知。需要延长保密期限的，应当在保密期限届满六个月前提出变更申请。

档案馆收到论文产生单位提交的变更申请表或项目来源单位的变更通知后，应当及时在载体原国家秘密标识附近作出变更标识，并标明变更后情况与变更时间。

3. 涉密学位论文解密

学校应当定期开展涉密学位论文的解密工作。对保密期限已满、解密时间已到或者符合解密条件，且未接到书面延长保密期限通知的，以及尚在保密期限范围内，但收到解除密级通知或正式公布的，档案管理人员应

当在载体原国家秘密标志附近作出解密标志，并注明解密时间。

解密后的研究生学位论文由档案馆按照内部资料进行管理。要求解密后公开的论文，导师或论文作者须将敏感内容去除后重新制作成可以公开的论文，按照公开学位论文要求再次提交图书馆以供开放利用。

四、科研成果新闻宣传的保密管理

做好高校科研成果宣传报道工作的保密管理，首先，要厘清高校科研成果新闻宣传报道形式；其次，依据规定准确界定科研成果是否涉密；最后，要做好科研成果新闻宣传报道的保密审查以及涉密成果对外宣传的保密审批，以确保国家秘密不从科研成果的发布途径泄露。

（一）职责与分工

按照“业务工作谁主管，保密工作谁负责”“自审与送审相结合”和“先审后用，先审后发”的原则，学校宣传部作为学校科研成果新闻宣传报道保密管理的归口管理部门，负责将保密管理要求融入各种形式的新闻宣传活动中，并组织实施；提供科研成果信息的部门负责对拟宣传信息的自审；科技处等业务归口管理部门负责对涉及武器装备科研生产事项以及涉及国家秘密界限不清的信息进行保密审查；发布科研成果信息的部门负责对拟发布信息的保密审查情况进行核查；保密管理办公室负责对校外信息发布部门提供保密审查意见。

（二）公开宣传报道的保密审查

科研成果新闻宣传报道的形式主要包括：①利用网站、微信、微博、博客、论坛等互联网媒介发布信息；②利用报纸、广播电视、声像制品、海报等传统媒介宣传报道；③通过论文著作投稿、专利申请、项目申报、成果报奖等活动向校外公开提供材料；④接受各类媒体、新闻出版单位采访报道等；⑤在校内外公开举办展览展示等。

科研成果新闻宣传报道不得涉及国家秘密，针对不同的科研成果宣传形式采用不同的保密审查方式。公开信息发布保密审查一般流程参见图 9-8。

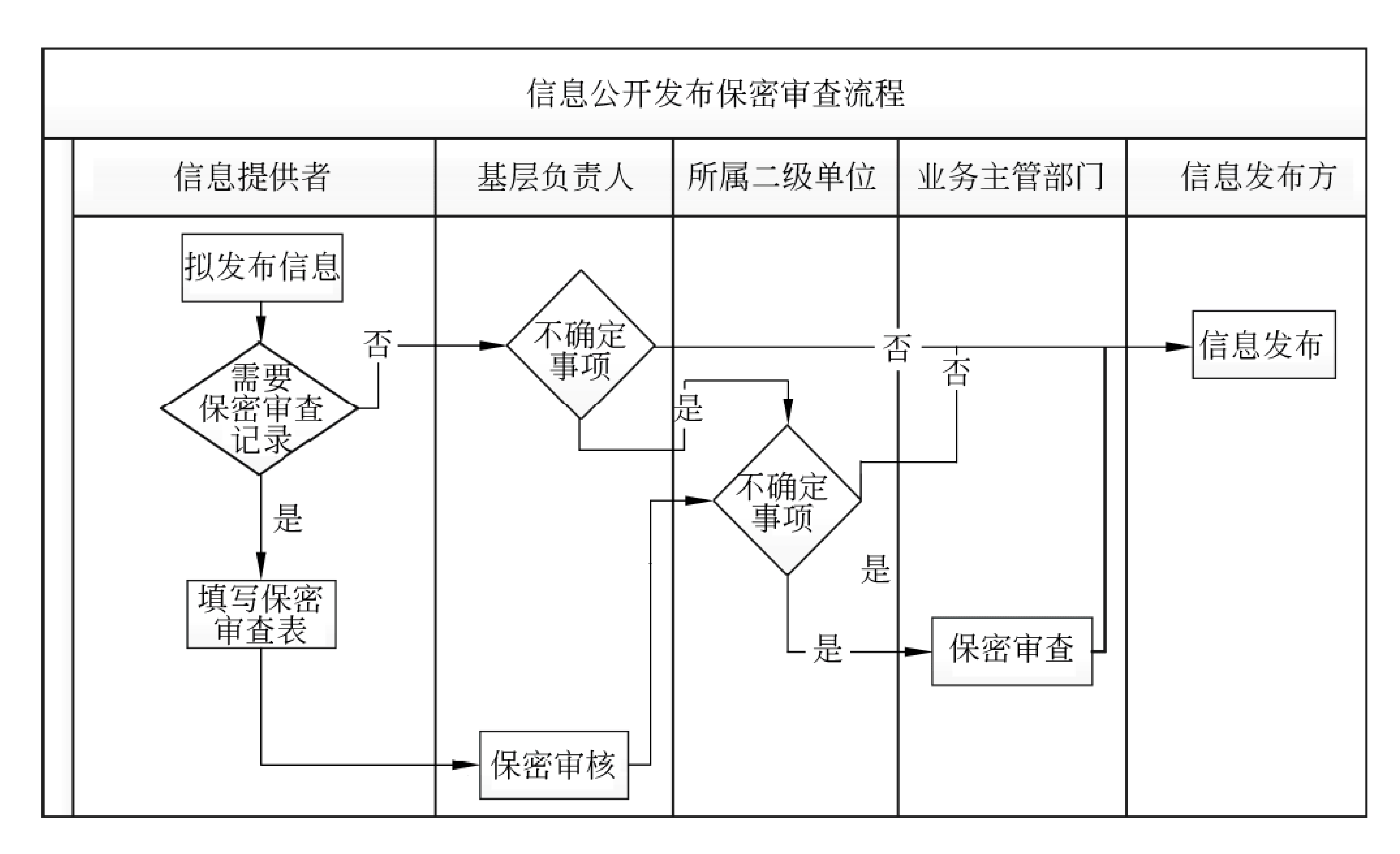


图 9-8　公开信息发布保密审查一般流程

1. 互联网媒介发布信息

互联网媒介是新闻宣传的主要途径，也是失泄密高发的主要源头。为了加强对互联网媒介信息发布的保密管理，应当从入口和出口两个方面严格执行保密审查制度。由基层单位负责人(科室负责人或项目负责人)对信息的提供者拟发布信息进行初步审核，经所属单位分管宣传工作的领导审核后发布。分管领导对审核的信息是否适合公开发布界定不清时，报本单位分管保密工作的领导或定密责任人审查，对是否属于涉密信息仍然把握不准的，报科技处等业务归口管理部门确定。未经保密审查的信息不得在学校管理的网站、公众号等信息发布平台上发布或转载。

鉴于高校各类信息发布量大，且主体业务不涉密国家秘密，各单位可以根据自身业务划定本单位可能涉及国家安全、国家利益和重大社会利益的事项，涉及上述有关事项的信息发布，必须履行保密审查流程。

学校师生、员工对以个人身份在微信、微博、博客、各种论坛上发布各种信息自行负责。

2. 传统媒介宣传报道

为了加强对出版社、电视台、报纸等传统媒介的保密管理，宣传部等业务归口管理部门应当组织有关单位，结合业务工作制定保密管理实施细则，明确禁止宣传报道的事项，对校内可能涉及国家安全、国家利益和重大社会利益的重点院系、重点人员（如涉密院系、知名专家、涉密人员等）提供信息时进行重点审查；对校外投稿人，要求提供稿件的同时，提供投稿单位保密管理部门出具的保密审查意见。

3. 论文著作投稿与专利申请

论文著作与专利是体现高校师生学术水平与学术成果的重要方面。涉密科研人员是涉密项目的参与者以及涉密事项的知悉者，而知名专家经常参与重大战略规划、国家政策研讨，也掌握大量敏感信息，可能在其论文著述及专利中涉及涉密或敏感信息。因此，应当对上述两类人发表论文或著作时进行重点的保密审查。

当前，不少高校在论文著作保密审查方面存在缺少主动性的现象，一般是文章或专著录用后，期刊或出版社要求学校出具保密审查意见时，才履行有关保密审查手续。为了提高师生们进行论文著作保密审查的积极性和主动性，可以采取以下对策：一是与财务报销制度联动，即未履行保密审查的论文专著，单位将不予报销版面费；二是与科研成果统计挂钩，未履行保密审查的论文专著，不计入科研成果统计范围；三是与单位保密考核结果挂钩，年度学术论文、专著保密审查率低于 90％的单位，保密考核不通过。

4. 公开申报材料

学校各业务归口管理部门在组织各院系申报公开项目、成果报奖等非涉密活动时，为了避免申报材料中涉及国家秘密事项或不宜公开的内部信息，推进保密管理与业务工作相融合，应当将保密审查环节融入项目、职务、报奖等各类申报材料审批过程中。材料接收单位要求学校出具保密审查意见的，由保密管理办公室根据学校有关管理流程予以出具（参见附表 9-8）。

5. 公开展览展示

主办或承办公开展览展示的单位（院系所等）负责对展览展示活动进行保密管理，展品一律不得涉密；当公开展览展示涉及武器装备科研生产事项时，还应当提交学校业务归口管理部门进行保密审查。展品来自校外单位时，要求其提供本单位保密管理部门出具的保密审查意见。

6. 公开媒体采访

校内外媒体采访统一由学校宣传部负责接洽，宣传部负责了解媒体采访意图及主要内容，并对接受采访人员进行保密提醒，必要时，征求业务归口管理部门意见（参见附表 9-9）。学校师生员工接受采访前，应当确认采访人员的工作身份，采访中禁止对外透露国家秘密信息或提供涉密文件资料。

（三）涉密成果宣传报道的保密审批

涉密科研成果的宣传报道形式主要包括涉密成果鉴定或报奖、举办涉密展览以及制作涉密声像制品等形式。涉密科研成果的宣传报道，应当履行审批程序，并制定保密方案或明确提出保密要求。

1. 涉密成果鉴定或报奖

学校所属各单位及个人申请国防专利、申报国防奖励或国防成果鉴定时，应当依据包含的涉密事项确定相应的材料密级，使用符合保密要求的设备制作，并明确标注密级。上级主管部门需要学校保密管理部门明确出具定密意见时，申报人持校内定密审批手续到学校保密管理办公室办理。

项目组成员脱密后如因申报国防专利、国防奖励或国防成果鉴定等活动需要处理或接触已结题项目涉密资料，可以参照非涉密人员查阅处理涉密信息流程处理。

2. 涉密展览

举办涉密展览时，应当按照规定上报上级主管部门审批。批准后，主（承）办单位应当制定保密工作方案，选择具备安全保密条件的场所，选择具有国家秘密载体印制资质的单位制作展品、展板并签署保密协议，指定专人负责展品制作、布置展室、接待参观等重要环节的保密管理工作，展览

结束后按照相关保密规定保存或者销毁展品、展板等涉密物品和资料。保密工作方案应当报学校保密管理办公室审批、备案，主（承）办单位与保密管理办公室应当对涉密展览的保密管理情况进行监督检查（参加附表 9-10）。

3. 涉密采访

因工作需要接受涉及武器装备科研生产事项等涉密事项的采访时，被采访单位和个人应当制定保密方案（参见附表 9-9），拟定采访安排，指定专人负责采访过程中所使用的设备及录像带、存储卡等存储介质的保密管理，明确采访素材的处理、审查和提供方式等。保密方案须经所在二级单位保密工作负责人审查同意后，报学校保密管理办公室审核备案。

附表 9-1　拟接触涉密信息非密人员资格审查表示例

拟接触涉密信息非密人员资格审查表

姓名		证件号		所在单位	
人员类型	□事业编制　□博士后　□合同制　□研究生　□退休　□外协				
本人与家庭成员情况					
本人有中华人民共和国国籍，且无国（境）外永久居留权、长期居留许可					是□　否□
本人与境外（含港澳台）人员无婚姻关系					是□　否□
是否存在配偶已移居国（境）外，或者没有配偶、子女均已移居国（境）外					是□　否□
其他情况					
是否因违反政治纪律受到过处分或者处罚					是□　否□
是否受过刑事处罚、被开除公职或者曾因严重违反保密规定被调离涉密岗位					是□　否□
本人、配偶及子女是否曾因危害国家安全的行为受到处分或者处罚					是□　否□
是否有吸毒、赌博等违法犯罪行为以及酗酒等不良嗜好					是□　否□
是否有泄密或造成重大泄密隐患情况					是□　否□
是否有针对本人利诱、胁迫、渗透、策反等特殊行为					是□　否□
本人承诺	1. 上述内容均属实，本人与家庭成员情况变化后 30 天内上报单位。 2. 如有虚假，自愿承担党纪政纪责任和法律后果。 承诺人：　　　年　月　日				
单位审查意见	□ 该同志符合涉密资格基本条件； □ 该同志可接触信息最高密级；　机密□　秘密□ □ 已对其进行保密教育提醒； □ 该同志已签署承诺书（附后）； □ 我单位承诺为其提供符合要求的涉密专用设备和存储介质； □ 同意其查阅处理涉密信息，凭证编号＿＿＿＿＿＿。 保密工作负责人签字：　　（公章） 年　月　日				

备注：配偶已移居国（境）外，或者没有配偶、子女均已移居国（境）外者，只限接触秘密级信息。

附件 9-2　非涉密人员查阅处理涉密信息保密承诺书示例

非涉密人员查阅处理涉密信息保密承诺书

本人因工作需要查阅处理涉密资料。为保守国家秘密，承诺按照学校、院（系、所）保密有关规定，遵守保密要求、履行保密责任：

一、严格控制知密范围，不向知密范围外的任何单位或个人以任何方式（直接、间接、口头或书面等）泄露所掌握的涉密信息；

二、严格遵守“涉密不上网，上网不涉密”，不利用各类网络传递转发所掌握的涉密信息；

三、撰写或处理涉密材料（含纸质文件和电子文档），利用单位提供的涉密设备、涉密存储介质；

四、制作、传递涉密载体严格履行手续，不通过普通邮政、快递等无保密措施的渠道传递涉密载体；

五、各类涉密载体（含摘录、撰写时产生的过程材料）妥善存放于保密柜中，使用完毕后及时交由院系集中保存或销毁，不私自丢弃、销毁、留存任何涉密载体。

六、如由本人造成泄密事件愿意承担纪律处分直至法律责任。

承诺人签字：

年　　月　　日

附件 9-3　非涉密人员查阅处理涉密信息凭证示例

非涉密人员查阅处理涉密信息凭证

______同志因工作原因需到你处查阅涉密信息。我单位已对其进行涉密资格审查、保密教育提醒，并签订保密承诺。现为其发放查阅凭证，编号：__________，可接触信息最高密级为：机密□　秘密□，有效期为：______年____月至______年____月。

请予接洽。

单位：

年　　月　　日

附表 9-4　涉密项目结题情况确认表示例

涉密项目结题情况确认表

<table>
<tr><td>申请脱密人员姓名</td><td></td><td>涉密岗位</td><td></td><td>所属单位</td><td></td></tr>
<tr><td colspan="6">作为涉密岗位承担者参与涉密项目情况</td></tr>
<tr><td>涉密项目
名称</td><td>项目编号</td><td>项目来源
1. 军口
2. 民口</td><td colspan="2">项目进展
情况(可多选)
1. 已验收
2. 经费到齐
3. 合同到期或终止
4. 已归档</td><td>项目负责人
签字确认
项目研制阶
段已结束,
不再形成新
的涉密资料</td></tr>
<tr><td></td><td></td><td></td><td colspan="2"></td><td></td></tr>
<tr><td></td><td></td><td></td><td colspan="2"></td><td></td></tr>
<tr><td></td><td></td><td></td><td colspan="2"></td><td></td></tr>
<tr><td colspan="6">本人承诺</td></tr>
<tr><td colspan="6">除以上项目外,本人未承担或参与其他涉密项目,也无正在申请的涉密项目
本人签字 :　　　　年　　月　　日</td></tr>
<tr><td colspan="3">院系审核意见</td><td colspan="3">科技处项目主管审核意见</td></tr>
<tr><td colspan="3">以上情况属实(　)
审核人:　年　　月　　日</td><td colspan="3">1. 以上项目名称、来源及进展情况属实
2. 其他:
审核人:　　　　年　　月　　日</td></tr>
</table>

附表 9-5　涉密协作配套单位保密监督检查表示例

涉密协作配套单位保密监督检查表

<table>
<tr><td>单位名称</td><td></td><td>法人代表</td><td colspan="2"></td></tr>
<tr><td>保密工作机构</td><td></td><td>保密机构负责人</td><td colspan="2"></td></tr>
<tr><td>项目名称</td><td></td><td>密级</td><td colspan="2"></td></tr>
<tr><td>项目起止时间</td><td></td><td>项目负责人</td><td colspan="2"></td></tr>
<tr><td>保密资格</td><td colspan="4">本单位保密资格等级__级，有效期：自____年__月__日至____年__月__日</td></tr>
<tr><td>监督检查方式</td><td colspan="4">□函调监督检查　　□现场监督检查</td></tr>
<tr><td>检查项目</td><td colspan="4">检 查 内 容</td></tr>
<tr><td rowspan="3">涉密人员</td><td colspan="3">是否按照规定对涉密人员进行资格审查、密级审定</td><td>□是 □否</td></tr>
<tr><td colspan="3">项目组涉密人员是否已报备并上交因私出国境证件</td><td>□是 □否</td></tr>
<tr><td colspan="3">对脱密人员是否清退涉密载体并办理脱密审批手续</td><td>□是 □否 □无</td></tr>
<tr><td rowspan="3">定密管理</td><td colspan="3">是否明确涉密事项的密级并控制知悉范围</td><td>□是 □否</td></tr>
<tr><td colspan="3">产生涉密电子文档、涉密资料是否规范标密</td><td>□是 □否 □无</td></tr>
<tr><td colspan="3">成果、专利等报奖材料申报是否准确定密或进行保密审查</td><td>□是 □否 □无</td></tr>
<tr><td rowspan="4">涉密载体</td><td colspan="3">涉密载体是否登记受控并建立台账</td><td>□是 □否</td></tr>
<tr><td colspan="3">涉密载体的制作、传递、借阅、使用、销毁是否符合规定</td><td>□是 □否</td></tr>
<tr><td colspan="3">涉密载体是否按照要求存放于密码文件柜</td><td>□是 □否</td></tr>
<tr><td colspan="3">项目结题验收后的资料是否按要求清理并归档</td><td>□是 □否 □无</td></tr>
<tr><td rowspan="3">涉密会议</td><td colspan="3">举办涉密会议的场所、使用设备是否符合保密要求</td><td>□是 □否 □无</td></tr>
<tr><td colspan="3">是否制定保密方案、指定专人负责</td><td>□是 □否 □无</td></tr>
<tr><td colspan="3">涉密会议资料发放是否编号登记并回收</td><td>□是 □否 □无</td></tr>
</table>

续表

信息设备	涉密设备及存储介质是否与互联网物理隔离	□是 □否 □无
	涉密计算机输出是否有审批登记	□是 □否 □无
	非涉密设备及存储介质是否存储处理涉密信息	□是 □否
失泄密事件	一年来是否发生过失泄密事件	□是 □否
协作配套单位承诺	本单位承诺对以上监督检查情况填报真实。 本单位承诺不断提高保密工作防范水平，确保国家秘密安全。 协作配套单位保密工作机构负责人签字： （公章） 年 月 日	
监督检查审核意见	项目组意见： 项目负责人签字： 年 月 日	
	保密管理办公室意见： 签字： （盖章） 年 月 日	

附表 9-6　研究生学位论文定密申请表示例

研究生学位论文定密申请表　　　　编号：

<table>
<tr><td>研究生姓名</td><td></td><td>学　号</td><td></td><td colspan="2">涉密人员
编号</td><td></td></tr>
<tr><td>导师姓名</td><td></td><td colspan="2">院（系、所）</td><td colspan="3"></td></tr>
<tr><td>论 文 题 目</td><td colspan="6"></td></tr>
<tr><td>论文（拟）开
题时间</td><td colspan="2">______年__ 月</td><td colspan="2">拟申请密级</td><td colspan="2">□　秘密______ 年
□　机密______ 年</td></tr>
<tr><td>论文来源
课题</td><td colspan="6">□校内：项目定密审批表编号：______________
□校外：提供校外单位保密监管承诺书
项目负责人：____________课题名称：____________________
密级：________________ 保密期限：_______ 年</td></tr>
<tr><td colspan="7">以上情况属实，本人承诺严格遵守研究生学位论文保密管理有关规定。

研究生签字：　　　　　　年　　月　　日</td></tr>
<tr><td colspan="7">申请论文保密的理由：

导师签字：　　　　　　年　　月　　日</td></tr>
<tr><td colspan="7">定密责任人审定意见：
定密责任人：　　　　　　年　　月　　日</td></tr>
<tr><td colspan="7">教务部门备案情况：
□已备案
教务部门主管：　　　　年　　月　　日</td></tr>
</table>

附表 9-7　校外单位保密监管承诺书示例

校外单位保密监管承诺书

<table>
<tr><td>研究生姓名</td><td></td><td>学 号</td><td></td><td>学 科</td><td></td></tr>
<tr><td>导 师 姓 名</td><td></td><td colspan="2">院（系、所）</td><td colspan="2"></td></tr>
<tr><td>论 文 题 目</td><td colspan="5"></td></tr>
<tr><td>论文来源课题</td><td colspan="5">课题来源单位：____________________
项目负责人：__________　课题名称：____________________
____
密级：__________　保密期限：____________年</td></tr>
<tr><td colspan="6">论文定密依据</td></tr>
<tr><td colspan="6">须说明论文与涉密项目的关系及该研究生参与该课题情况：

项目负责人签字：　　　　年　月　日</td></tr>
<tr><td colspan="6">课题来源单位保密承诺</td></tr>
<tr><td colspan="6">须详细说明对论文作者、撰写论文所使用设备、与论文相关的电子、纸介质载体是否按照涉密人员、涉密设备、涉密载体的要求进行管理。

保密负责人签字：　　　　（单位公章）
年　月　日</td></tr>
</table>

附表 9-8　申报材料保密审查表示例

申报材料保密审查表

<table>
<tr><td>申请人姓名</td><td></td><td>所在单位</td><td></td></tr>
<tr><td>申报材料
名称或内容</td><td colspan="3"></td></tr>
<tr><td>材料去向</td><td colspan="3"></td></tr>
<tr><td>申请人自审</td><td colspan="3">材料是否涉及涉密科研项目　是（　）　否（　）

签字：　年　月　日</td></tr>
<tr><td>课题负责人
审查意见</td><td colspan="3">以上情况是否属实　是（　）　否（　）
是否同意申报　是（　）　否（　）

签字：
年　月　日</td></tr>
<tr><td>所在单位保密
审查意见</td><td colspan="3">是否同意申报　是（　）　否（　）
提交业务主管部门审核（材料存在不明事项或涉及涉密科研项目时）
是（　）　否（　）

负责人签字：　（单位公章）
年　月　日</td></tr>
<tr><td>业务主管部门
审查意见</td><td colspan="3">（材料存在不明事项或涉及涉密科研项目时）
是否同意申报　是（　）　否（　）

负责人签字：　（单位公章）
年　月　日</td></tr>
</table>

附表 9-9　接受采访保密审查表示例

接受采访保密审查表

接受采访人		所在单位	
联系方式		接受采访人身份	涉密人员　是□　否□
接受采访时间	年　月　日　午　时　分　星期（　）		
拟发布媒体名称		拟发布时间	
发布形式	□新闻稿　□图片　□视频　□其他＿＿＿＿		
事项类别	（涉密人员必填） 涉及武器科研生产事项　是□　否□ 涉及党政事项　是□　否□ 涉及其他涉密事项　是□　否□		
审查内容：（采访方案及安排请附后，**涉及涉密武器装备科研生产事项等涉及国家秘密事项的采访，应制定保密方案，报保密办审核备案**）			
所在单位意见	经审查，□ 采访内容不涉及国家秘密事项 □ 采访内容涉及国家秘密事项 □ 存在不明确事项 单位负责人签字（公章）：　年　月　日		
业务主管部门意见	（存在不明事项或涉及武器装备科研生产事项时由业务主管部门审查） 单位负责人签字（公章）：　年　月　日		
宣传部审批意见	签字（公章）：　年　月　日		

附表 9-10　涉密展览保密监督检查表示例

涉密展览保密监督检查表

<table>
<tr><td>主(承)办单位名称</td><td></td><td>展览名称</td><td></td></tr>
<tr><td>主(承)办单位负责人</td><td></td><td>联系电话</td><td></td></tr>
<tr><td>监督检查方式</td><td colspan="3">□主(承)办单位监督检查　□保密办监督检查</td></tr>
<tr><td>检查项目</td><td colspan="3">检查内容</td></tr>
<tr><td>展览密级</td><td colspan="3">□ 一般涉密展览　□ 重要涉密展览</td></tr>
<tr><td>组织机构及职责</td><td colspan="3">1. 主管部门领导是否对展览安排进行指导和监督　□是□否
2. 主(承)办单位是否向保密办咨询相关要求　□是□否
3. 是否制定展览的安全保密方案　□是□否
4. 是否指定安全保密负责人保障展览安全保密工作　□是□否</td></tr>
<tr><td>涉密展览管理情况</td><td colspan="3">5. 是否确定工作人员范围　□是□否
6. 是否对工作人员进行保密审查,签署保密承诺书　□是□否
7. 是否明确参观范围和人员管控措施　□是□否
8. 是否对参观人员进行政治审查和保密教育　□是□否
9. 是否履行涉密展览签到手续　□是□否
10. 展厅技防措施是否落实并运转正常　□是□否
11. 是否安排专人 24 小时值班　□是□否
12. 展品的运输是否符合保密要求　□是□否
13. 展品是否明确数量并指派责任人和专人管理　□是□否
14. 展厅是否符合保密要求,监控是否未正对涉密展品　□是□否
15. 文件资料是否履行编号登记发放手续　□是□否
16. 展览结束后是否认真履行清点、登记、销毁工作　□是□否
18. 涉密展览是否允许录音　□是□否
19. 录音是否经展览主管部门的领导批准并明确责任人　□是□否
20. 涉密展览是否使用各种无线设备　□是□否
21. 涉密展览是否有涉密视频播放　□是□否
22. 涉密视频制作和播放是否符合保密要求　□是□否
23. 涉密展览的解说是否经保密审查,符合保密要求　□是□否
24. 展览是否开启移动通信干扰器或信号屏蔽装置　□是□否
25. 参加展览人员是否将手机带入展场　□是□否
26. 展览结束后,是否对展场进行安全检查　□是□否</td></tr>
<tr><td rowspan="3">检查方</td><td colspan="3">展览负责人签字:</td></tr>
<tr><td colspan="3">主(承)办单位领导签字:</td></tr>
<tr><td colspan="3">保密办签字(重要涉密展览需此项):</td></tr>
</table>

第十章　保密检查与奖惩

保密检查是高校科研保密管理的重要组成部分,是深入开展保密宣传教育、强化安全保密意识的重要媒介,是依法推进保密工作的重要手段,也是发现和消除泄密隐患的重要途径。为了确保保密检查的有效性,检查结果应当与涉密单位开展人员考核和实施奖惩等工作相结合。

一、保 密 检 查

保密检查主要是指学校保密工作机构(保密管理办公室)及相关业务归口管理部门、各涉密院系等基层单位依据国家保密法律、法规和有关标准与指南,采取相应的管理和技术手段,对相关单位及人员落实保密责任制和执行保密规章制度的情况进行检查的活动。

(一)职责与分工

学校保密管理办公室负责制订学校年度保密检查工作计划,组织实施校级保密检查,根据需要会同有关业务归口管理部门,组织对重点领域、重大专项、特定工作的保密专项检查,监督指导学校各涉密单位的保密自查,配合上级机关、相关单位完成有关检查工作;各涉密单位负责按季度组织开展本单位保密自查。

(二)保密检查工作计划

为了使保密检查工作更具计划性,每年年初或春季学期初,学校保密

管理办公室应当依据保密检查工作要求、学校年度保密工作重点以及单位存在的主要保密风险等，制订学校年度保密检查计划，对本年度学校的保密检查时间、内容、范围等做出安排，并根据情况变化及时调整。

1. 保密检查要求

保密检查要求主要来源于以下几个方面。

（1）《武器装备科研生产单位保密资格认定办法》中提出的保密检查要求，主要包括：学校每学期开展一次全校性的综合检查，结合实际工作每年开展1～2次专项保密检查，对发现的问题提出书面整改要求，并督促整改；学校所属的各涉密单位每季度进行一次保密自查，自查及整改情况报单位保密工作机构。

（2）国家及所在地区保密行政管理部门、教育部、国防科工局等上级机关、单位结合当前保密形势布置的保密检查要求，如涉密项目保密检查、信息安全保密检查、专门设备保密检查等。

（3）上级业务主管部门结合业务工作布置的保密检查要求，如相关军口项目管理部门布置的针对某类项目的专项保密检查。

2. 保密检查内容

保密检查内容一般包括：

（1）基层保密工作组织机构设置和人员配备情况、涉密人员培训教育与管理情况；

（2）定密工作开展情况、国家秘密载体与密品管理情况；

（3）信息系统、信息设备和存储设备保密管理情况；

（4）互联网使用保密管理情况；

（5）保密技术防护设施、设备配备使用情况，涉密场所保密管理情况；

（6）协作配套、涉密会议、新闻宣传、涉外活动等保密管理情况；

（7）保密检查、考核、奖惩与保密工作责任制落实情况等。

为了使保密检查更具针对性，应当根据每次检查要求和被检查单位的具体情况安排检查内容。例如，对例行综合检查，检查内容应当尽可能全面，但对不同涉密部门，可以结合其近期开展的主要科研活动和日常管理

与监督检查发现中的问题,设计重点检查内容,各单位的检查侧重点可以不同,可偏重涉密场所管理、脱密人员管理的检查,也可重点检查单位的非涉密信息设备情况,还有的单位可重点检查其协作配套与外场试验管理情况等。

3. 保密检查范围

保密检查的范围应当依据每次检查的要求划定,针对半年一次的综合检查,检查范围应当覆盖学校保密管理体系的所有部门;针对专项检查,则根据检查内容和涉及单位确定,比如上级业务主管部门布置的针对某类项目的保密检查,检查范围就限定在承担这类项目的院系和课题组。

4. 保密检查形式

学校及各涉密单位可以根据实际情况和需要,采取集中检查与日常监督检查相结合,联合检查与技术检查相结合,通知检查与飞行检查相结合,利用自查、互查、抽查及复查等方式开展综合检查或专项检查。

(三)保密检查实施

一次完整的保密检查活动一般包括制定保密检查方案,组织实施保密检查,对检查发现问题组织整改并跟踪验证以及总结汇报等内容,保密检查工作流程参见图 10-1。

1. 制定检查方案

保密管理办公室根据年度保密检查计划,提前制定检查工作方案,成立检查组,确定检查组长及成员,明确检查时间、检查范围、抽查对象和检查内容,设计保密工作检查记录单(参见附表 10-1),并将检查安排与检查组成员通知受检单位。

检查组成员应当是涉密人员,应当熟悉保密工作业务,了解受检单位的保密工作基本情况,明确检查内容与相关工作要求等。

各受检单位的抽查对象根据其涉密等级、承担任务数量与规模、遵守保密规章制度情况以及上次受检时间间隔等因素综合确定。

常用的保密检查方法包括要素检查法与过程检查法。要素检查法是指以保密管理要素为关注点,针对不同管理要素,根据受检单位或受检人

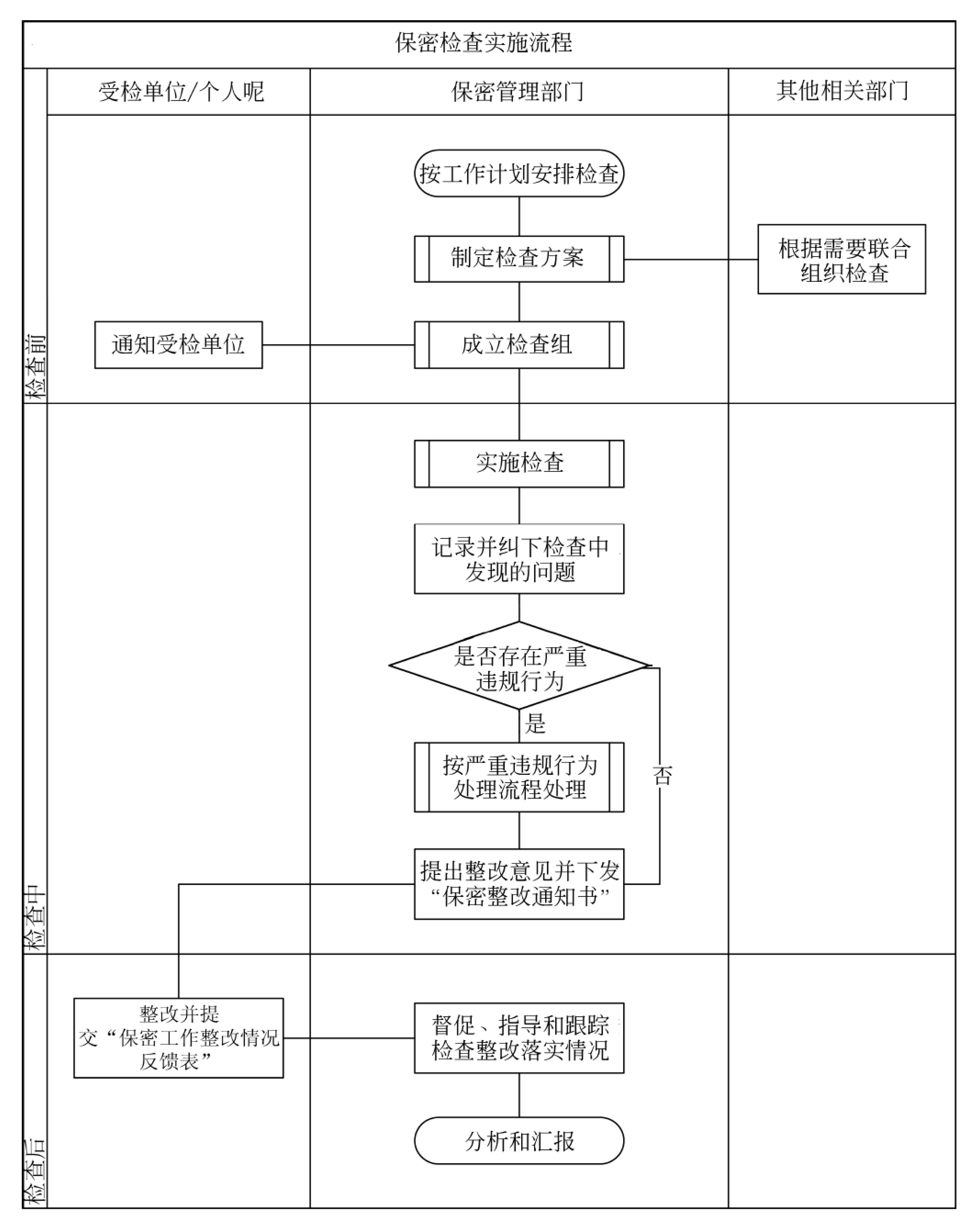


图 10-1　保密检查工作流程

员提供的相关资料、设备，实施的检查。过程检查法是指以项目执行过程为主线，以项目定密为源头，结合项目合同书或任务书内容，检查参与的涉

密人员、产生的涉密载体、使用的信息设备、举办或参与涉密会议以及协作配套、外场试验等项目执行过程中涉及的保密管理要素以及各种涉密活动的保密管理情况。相对而言,过程检查法更容易发现问题,因而更适用于保密体系相对成熟的单位。

保密检查应当运用必要的保密技术检查装备和手段,相关装备应当符合国家相关保密规定和标准,并经国家保密行政管理部门授权的检测机构检测通过。

2. 实施保密检查

检查人员按照检查工作方案实施检查,在保密工作检查记录单中详细记录检查结果,指出并纠正检查中发现的问题。受检单位或个人应当按照保密检查要求,积极予以配合,如实反映情况,提供必要资料。对检查结果,由相关各方签字确认。

如在保密检查中发现严重违规违纪行为或者失泄密隐患的,检查组应当当场责令受检单位停止使用或者封存有关设施设备、场所和载体等,并及时向学校保密管理办公室报告。责令停止使用或者封存的有关设施设备和载体等应当保持存储信息原始状态,学校保密管理办公室组织相关单位对其进行取证分析,必要时还应当按规定进行保密技术检测。

3. 整改与验证

现场检查结束后,学校保密管理办公室针对检查发现的问题向受检单位提出整改意见并下发保密整改通知书(参见附件 10-2);受检单位应当按照整改通知书的要求,在限定时间内制定整改方案,按期整改,并向保密管理办公室提交整改情况反馈表(参见附表 10-3)。

学校保密管理办公室对受检单位的整改落实情况进行跟踪检查,对已落实整改要求的作出整改结论,对未落实整改要求的提出进一步处理意见。

4. 总结与汇报

学校保密管理办公室应当及时对检查情况、检查结果及整改情况进行汇总分析,定期向学校保密委员会汇报,必要时以会议或简报等形式在学校各涉密单位内部进行通报。

（四）各涉密单位保密自查

学校各涉密单位的保密自查工作由本单位保密工作领导小组按季度组织实施，可以参照学校保密检查的实施流程进行自查和整改实施工作（参见附表10-4），自查与整改情况记录作为本单位保密检查工作档案留存，并将自查及整改情况报学校保密管理办公室。

（五）保密风险评估

学校保密管理办公室应当结合日常管理、监督指导与保密检查情况，定期进行全校保密风险评估，提出改进建议，报学校保密委员会审批。保密委员会研究讨论后确定改进措施，由保密管理办公室负责督促落实，持续推进学校保密工作的改进。

保密风险评估可以单独进行，也可以包含在年度保密工作总结中。

二、泄密事件报告和查处

泄密事件是指违反保密法律、法规，使国家秘密被不应知悉者知悉，或者超出限定的知悉范围，而不能证明未被不应知悉者知悉的事件。属于国家秘密的文件、资料或其他物品下落不明的，自发现之日起，绝密级十日内，机密、秘密级六十日内查无下落的，按泄密事件处理。

对泄露国家秘密事件进行报告和查处，其目的在于及时发现隐患，查补漏洞，减少损失，维护国家安全利益。

（一）职责与分工

学校保密委员会负责审议针对有关责任人的处理意见，审批泄密事件上报材料；学校保密管理办公室负责具体落实泄密事件报告和查处工作；发生泄密事件的单位和责任人应当配合泄密事件的查处。

（二）泄密事件报告

泄密事件实行一事一报的逐级报告制度。发生/发现泄密事件的单位或个人应当按照报告的程序在规定时间内逐级上报，不得隐瞒、拖延报告或自行处理后再报告。报告的时限、程序及主要内容如下（参见附表 10-5）：

1．报告时限与程序

发生泄密事件的单位，发现后应当立即向学校保密管理办公室口头报告，对危害进行初步评估，在保护好现场的同时采取紧急补救措施，以挽回或减少泄密造成的损失，并 12 小时内书面报告学校保密管理办公室。

学校保密管理办公室发现泄密事件或接到泄密事件报告后，应当立即进行情况核实，在初步核实的前提下，向学校保密委员会领导汇报，对泄密事件造成的后果要及时进行危害评估，提出补救措施和查处方案建议，并在 24 小时内书面向教育部等上级主管部门和所在地区的国家保密行政管理部门报告。发生机密级以上重大泄密事件，同时向国家保密局报告。情况紧急时，应当先口头报告简要情况。

2．报告主要内容

报告泄密事件，一般应当包括以下内容。

（1）被泄露国家秘密事项的内容、密级、数量及其载体形式。

（2）泄密事件的发现经过。

（3）泄密责任人的基本情况。

（4）泄密事件发生的时间、地点及经过。

（5）泄密事件造成或可能造成的危害。

（6）已进行或拟进行的查处工作情况。

（7）已采取或拟采取的补救措施等。

（三）泄密事件的查处

泄密事件查处工作是指对泄密事件的调查和处理。主要工作内容包括：①查明所泄露国家秘密事项的内容、密级、危害程度，主要情节和有关

责任者等。②采取必要的补救措施。③根据国家的有关法律、法规或规定，对泄密责任人提出处理意见，并做出处理。情节严重的交由国家司法机关处理。④针对泄密事件暴露出的问题，提出整改和加强保密工作的意见。

泄密事件的查处工作坚持实事求是和依法办事的原则。

1. 泄密事件调查

一般泄密事件由学校保密管理办公室负责调查，上级主管部门和有关保密行政管理部门对调查工作进行监督；重大泄密事件由上级主管部门和有关保密行政管理部门直接进行调查，学校保密管理办公室协助配合。泄密事件调查中，需要查明：

（1）被泄露国家秘密事件的具体内容、密级、数量。

（2）已经或可能造成的危害及危害程度。

（3）是否可以补救以及可以补救的措施。

（4）事件发生、发现的经过及主要情节。

（5）对事件性质的认定。

（6）当事人的基本情况及对事件应负的责任。

（7）应采取的改进措施或加强保密工作的意见等。

2. 泄密事件处理

对泄密事件责任人或事件有关责任人处罚的种类包括刑事处罚、党纪政纪处分、罚款和通报批评等。在查明泄密事件的基础上，学校保密管理办公室依据学校保密考核与奖惩办法提出具体的处理意见，报保密委员会审批后执行。对需要追究责任人刑事责任的，立即将案件移交有关国家机关处理。

3. 泄密事件查处结果报告

学校须在发生泄密事件后三个月内完成查处工作，并向学校上级主管部门和行政管理部门书面报告泄密事件查处结果。报告的内容一般包括以下几点：

（1）泄密事件的发生、发现过程。

（2）泄密事件已经或可能造成的危害。
（3）造成泄密事件的主要原因和教训。
（4）对有关泄密责任人的处理情况。
（5）采取的补救措施和加强保密工作的情况等。
因特殊情况在规定时间内查处工作未能结案或未能报告查处结果的，应当在规定时限内报告查处进展情况和未查结的原因。

三、考核与奖惩

保密工作虽然不是高校的核心工作，但会对教学、科研等工作产生直接影响。为了推动保密工作责任的落实，一方面，需要将相关涉密单位保密工作的开展情况纳入学校年度绩效考核，有关岗位人员（包括学校党政主要领导、分管保密工作校领导、与科研保密工作密切相关的其他校领导、涉密单位负责人、项目负责人、涉密人员等）履行保密职责情况与个人年度绩效工资挂钩。另一方面，学校应当每年对保密工作做出成绩的部门和个人给予表彰奖励，形成推动保密工作落实的良好氛围。同时，要对违反保密规章制度或者不履行保密责任的直接责任人和相关责任人给予处罚，严格执行保密工作责任追究制度。作为一种管理手段，考核与奖惩目的是让涉密人员增强保密意识，提高岗位责任感和行为自觉性，促进保密工作习惯养成。

（一）保密工作考核

高校保密工作一般以自然年度为周期进行考核，考核范围包括学校各级保密工作负责人和涉及保密工作的单位及相关人员。为了推进保密工作与业务工作融合，应当将保密责任履职情况纳入学校各单位、各级各类人员的考核内容。保密工作考核应当坚持“实事求是、客观公正、标准明确、奖罚分明”的原则。

1. 职责与分工

学校人事处负责制定学校所属各单位的年度考核评估办法，将相关涉

密单位开展保密工作的情况纳入考核评估内容，并会同保密管理办公室组织开展各涉密单位和涉密人员的保密工作考核；组织部负责将保密工作开展情况纳入各单位领导班子的年度考核内容；各涉密单位负责落实本单位涉密人员保密工作考核。

2. 学校党政领导班子和班子成员保密工作考核

学校党政领导班子和主管、分管保密工作校领导及其他负责人年度述职时，述职内容应包含学校或分管业务保密工作总体情况以及保密工作领导责任制落实情况。

3. 涉密单位领导班子和班子成员保密工作考核

对各涉密单位领导班子和班子成员保密工作考核的主要内容有以下几点：

（1）各类保密工作会议的参会情况。

（2）保密管理责任制的落实情况。

（3）对分管保密业务工作的熟悉情况。

（4）分管保密业务工作的落实情况。

（5）实际保密管理工作的成效等。

各涉密单位领导班子与成员在干部考核述职时，应当对履行保密管理职责的情况进行述职。学校组织部应当把各涉密单位领导班子与成员履行保密责任的情况纳入年度绩效考核内容。保密管理办公室应该将对涉密单位保密负责人的考核结果(参见附表10-6)报组织部备案。

4. 涉密单位和涉密人员保密工作考核

对各涉密单位保密工作考核的主要内容有：

（1）保密管理组织机构的建立及各级保密管理责任制的落实情况。

（2）执行学校保密规章制度的情况及本单位保密规章制度的建设情况。

（3）保密宣传教育情况。

（4）涉密人员管理情况。

（5）国家秘密载体管理情况。

（6）保密要害部门、部位管理及防护措施情况。

（7）信息系统、信息设备和存储设备等安全保密管理情况。

（8）重大涉密、涉外活动保密保障工作情况。

（9）保密自查的落实情况与保密工作档案建设情况等。

对于学校各涉密单位保密工作考核，可采取单位自评和业务归口部门综合考核相结合的方式。每年年终时，各单位根据保密工作落实情况进行保密工作年度总结，在此基础上形成保密工作自评报告，报学校保密管理办公室。保密管理办公室会同相关业务归口部门，结合各涉密单位的日常保密工作开展情况、校级保密检查结果及整改落实情况和保密工作自评报告等，对各单位进行年度保密工作综合考核（参见附表 10-7），考核结果报保密委员会审批，纳入各单位年度总结评估依据。

5. 涉密人员保密工作考核

对涉密人员考核的主要内容有：

（1）政治思想及工作表现。

（2）对保密法律、法规、基本知识、规章制度的掌握知悉情况。

（3）执行保密法律、法规、规章制度的情况。

（4）参加保密教育培训情况。

（5）配合保密领导组完成保密工作任务的情况等。

涉密人员保密工作考核（参见附表 10-8）的由各单位保密工作领导小组组织，并将本单位涉密人员年度考核结果上报人事处与学校保密管理办公室。

6. 考核结果与绩效奖励

学校保密工作考核结果一般包括优秀、合格与不合格三种情况。考核优秀的单位数量一般占学校全部涉密单位一定比例（10％～20％）。有下列情形之一的，视为考核不合格：

（1）擅自与境外（含港澳台）组织、机构或者个人合作开展涉密业务的。

（2）擅自聘用境外（含港澳台）人员从事涉密业务的。

（3）出租、转让、转借、篡改保密资格证书的。

（4）存在重大泄密隐患经警告逾期不改的。

（5）发生泄密事件隐瞒不报的。

（6）发生泄密事件，未进行整改或者整改措施不落实的。

（7）严重违反保密规定，发生重大泄密事件的。

保密工作实行一票否决制，保密工作考核不合格的单位及个人，学校年度综合考核不合格。

为了进一步推进落实保密责任制，各涉密单位、保密工作各级负责人与涉密人员的保密工作考核结果应当与绩效工资挂钩。保密工作考核优秀的单位，绩效工资在平均值基础上上浮一定比例（如10％）；考核不合格的，绩效工资在平均值基础上下浮一定比例（如10％～20％）甚至停发年度绩效工资，同时取消当年单位评优资格。

考核优秀人员，个人年度绩效工资在平均值基础上上浮一定比例（如20％）；考核不合格者，个人年度绩效工资在平均值基础上下浮一定比例（如50％），甚至停发年度绩效工资，同时取消当年学校各类评优资格，并采取降低下一年度岗位津贴等级处理。为了更有效地激励涉密人员，对考核优秀或合格的涉密人员应当在单位职务晋升以及个人评优中给予政策倾斜。

（二）保密奖励

学校一般设立保密工作先进集体、保密工作先进个人以及各类专项奖等奖项，对在保守、保护国家秘密以及改进保密技术、措施等方面成绩显著的单位或者个人予以表彰奖励。

1．职责与分工

学校保密委员会作出表彰和奖励决定；学校保密管理办公室负责组织推荐和评选；各涉密单位负责推荐候选基层单位与候选人。

2．保密工作先进集体的评选条件

保密工作先进集体面向学校各涉密单位以及项目组进行评选，参评条件主要包括以下几点：

（1）对本单位（项目组）涉密人员经常开展保密教育，及时学习保密工作相关方针政策和保密法律法规以及学校保密规章制度。

（2）能够按时完成上级和学校的各项保密工作任务，并结合本单位（项目组）的实际情况创造性地开展保密工作，成绩突出。

（3）保密工作责任明确，保密防范措施到位，保密管理规范。

（4）近三年内本单位（项目组）未发生失泄密事件，未发现严重的保密安全隐患，内部工作人员未因保密原因受到纪律处分。

3. 保密工作先进个人评选条件

保密工作先进个人面向涉密人员进行评选，参评标准主要包括以下几点：

（1）在涉密工作岗位或保密管理工作岗位上连续工作一年以上，保密工作年度考核优秀。

（2）认真学习并贯彻落实保密工作相关方针政策和保密法律法规以及学校保密规章制度，积极参加保密教育培训，具有较强的保密意识和防范能力。

（3）熟悉本职工作中的涉密事项和保密工作重点，保密工作成绩突出或作出特殊贡献。

（4）近三年内未受到纪律处分，无违反保密法律法规以及学校保密规章制度的行为。

参评人员为单位保密工作负责人（如涉密项目负责人）的，本单位（项目组）还应当三年内无失泄密事件，保密工作成绩突出。

4. 保密专项工作奖评选条件

凡在工作中一贯严格遵守国家保密法律、法规和学校保密规章制度，从未发生失泄密事件的，且符合下列条件之一的，学校可设置专项奖予以表彰：

（1）在涉密专项活动中，积极主动、成绩突出或者作出特殊贡献的。

（2）对改进保密管理工作提出合理化建议，为加强保密技术管理作出显著贡献的。

（3）发现他人泄露或可能泄露国家秘密，立即制止和采取补救措施，避免或者减轻损害后果的。

（4）在危急情况下，保护国家秘密安全或对侦破失泄密案件有重大贡献的。

5. 评选程序

一般包括确定奖励方案、组织评选与审议评选结果等环节。

（1）学校保密管理办公室拟定保密奖励方案，提出推荐比例和评选名额，报学校保密委员会审批。

（2）各单位按照奖励方案和明确的评选条件，推荐候选单位和个人（参见附表 10-9、附表 10-10）。

（3）保密管理办公室组建评审小组，召开评审会，组织评选。

（4）评选结果报保密委员会审议，决定表彰名单。

6. 奖励周期与形式

学校保密工作先进集体与个人奖励活动，原则上每年评选一次。专项奖励一般在组织开展涉及单位多、持续周期长、影响重大的专项保密活动（如保密认定工作）时设置。保密工作奖励以荣誉奖励为主，物质奖励为辅。

为了更充分调动涉密人员保密工作的积极性，学校鼓励各涉密单位在本单位内部开展保密工作表彰奖励活动。对上级主管机关及各级政府部门设立的保密表彰奖励，一般由学校保密管理办公室根据学校表彰奖励情况择优推荐上报名单，经学校保密委员会审定后，由保密管理办公室组织申报。

（三）保密工作责任追究

学校各级保密工作负责人和涉密人员如违反国家保密法律法规以及学校保密规章制度或者不履行保密责任的，学校应当视情节对直接责任人和相关责任人进行责任追究。

1. 职责与分工

学校保密委员会决定学校保密工作的相关责任追究事项；保密管理办

公室负责具体组织落实。

2. 直接责任人问责

根据《中华人民共和国保守国家秘密法》和《武器装备科研生产单位保密资格认定办法》和学校保密管理规定，对学校或上级机关保密监督检查中发现有关违法违规行为问责，视情节轻重，对相关责任人员进行约谈、责令作出书面检查直至通报批评，依纪依法给予党纪政纪处分；构成犯罪的，依法追究刑事责任等（参见附件 10-11、附件 10-12）。

3. 相关责任人问责

对因领导履行保密工作责任制不力，致使职责范围内发生泄密事件的，还应当对责任部门相关负责人进行保密问责（参见附件 10-13）。因保密部门监管不力、工作失职发生重大失泄密事件的，给予保密部门负责人必要的处分和经济处罚。

对举报泄露国家秘密或违反保密规定的检举人进行打击报复的，给予行政记过及以上处分，并处经济处罚，直至移交司法机关追究刑事责任。

处理决定以书面形式通知本人及所在单位，并视情节在一定范围内通报。

附表 10-1　保密检查工作记录单(部分项目)示例

保密检查工作记录单(部分项目)

检查项目	国家秘密载体管理		
检查单位		检查时间	
被检查人员			
序号	检 查 内 容		检查结果
1	涉密载体(含介质)是否有台账,是否账物相符		是□　否□
2	涉密载体是否表明密级、保密期限		是□　否□
3	涉密文件制作是否编排顺序号、打印是否审批登记		是□　否□
4	收发、传递、借阅、使用、保存、销毁是否符合国家规定		是□　否□
5	过程文件资料管理是否符合要求		是□　否□
6	复印涉密载体有无审批登记记录		是□　否□
7	涉密载体维修、报废是否符合国家有关保密规定		是□　否□
8	涉密载体的存放是否符合有关规定		是□　否□
9	是否根据工作需要控制了国家秘密载体的知悉范围		是□　否□

检查中发现的问题:

检查组:　　　　　　　　　　　　　　　　被检查方代表:

续表

检查项目	非密办公计算机、外网计算机管理		
检查单位		检查时间	
被检查人员			
序号	检 查 内 容		检查结果
1	非密办公计算机和上网计算机是否有台账，账物是否相符，是否有标识		是□ 否□
2	非密办公机是否有上网记录，是否处理、存储涉密信息的信息		是□ 否□
3	非密办公计算机是否安装了杀毒软件，杀毒软件是否为开机自动运行		是□ 否□
4	非密办公计算机有无涉密介质连接记录		是□ 否□
5	有无将个人计算机及存储介质带入单位使用		是□ 否□
6	外网计算机是否落实责任人		是□ 否□
7	外网计算机是否有处理、存储涉密信息，是否有涉密存储介质接入记录		是□ 否□
8	外网计算机身份认证系统是否有效		是□ 否□
9	网上发布信息是否有审查审批记录		是□ 否□
10	外网计算机是否安装了杀毒软件，病毒库是否自动升级，杀毒软件是否为开机自动运行，是否定期全盘杀毒		是□ 否□

检查中发现的问题：

检查组： 被检查方代表：

续表

检查项目	涉密计算机和涉密存储介质的管理		
检查单位		检查时间	
被检查人员			

序号	检 查 内 容	检查结果
1	涉密计算机和涉密存储介质是否有台账，是否账物相符	是□　否□
2	涉密计算机和涉密存储介质是否已按要求粘贴标识	是□　否□
3	涉密计算机有无上网记录，是否有非涉密介质连接记录	是□　否□
4	涉密计算机是否已设置安全策略，是否已设置账户策略，密码长度、复杂性更换期限是否符合规定	是□　否□
5	涉密计算机是否设置符合要求的 bios 密码、系统密码、屏保密码，屏保启动时间 10 分钟内，是否按规定时间更换密码	是□　否□
6	涉密计算机是否安装了杀毒软件，病毒库是否按照规定升级，杀毒软件是否为开机自动运行	是□　否□
7	涉密计算机内所有涉密电子文档是否按规定要求标密，且正文与首页不分离	是□　否□
8	凡是从网络或其他途径获得的信息是否经中间机杀毒后刻录一次性光盘输入涉密计算机	是□　否□
9	涉密机是否使用电磁泄漏防护电源插座供电，且未与外网机、传真机等非涉密设备公用	是□　否□
10	涉密机网卡、蓝牙等是否拆除	是□　否□
11	涉密机是否与外网和非密设备实行了物理隔离，距离 1 米以上	是□　否□
12	涉密载体是否做到相对集中输出，是否有审批、登记记录	是□　否□
13	携带涉密便携机及存储介质外出，是否经领导审批	是□　否□
14	便携机带出前，返回后是否进行了保密检查	是□　否□
15	是否使用未经审批的涉密笔记本存储涉密信息	是□　否□

检查中发现的问题：

检查组：　　　　　　　　　　　　　　　　被检查方代表：

附件 10-2　保密整改通知书示例

保密整改通知书

编号：

__________：

在　　　年　　月　　日的____________________检查中，发现你单位存在以下问题：

____

____

____

根据保密法律法规和学校管理制度要求，现责成你单位按学校保密有关规定进行整改。在本通知书下达之日起____个工作日内，就本单位所存在的问题制定整改方案、落实整改措施，填写《保密工作整改情况反馈表》，报校保密办。

保密办将根据需要，在收到反馈后的____个工作日内对整改情况进行验证。

特此通知。

＊＊大学保密管理办公室

年　　月　　日

附表 10-3　保密工作整改情况反馈表示例

保密工作整改情况反馈表

<table>
<tr><td>单位</td><td colspan="2"></td><td>整改通知书编号</td><td></td></tr>
<tr><td colspan="5">原因分析及整改措施</td></tr>
<tr><td colspan="5"></td></tr>
<tr><td colspan="5">整改措施落实情况及举一反三检查情况</td></tr>
<tr><td colspan="5"></td></tr>
<tr><td colspan="2">单位保密领导
小组审核意见</td><td colspan="3">签字(公章)：
年　月　日</td></tr>
<tr><td colspan="2">整改情况
有效性验证</td><td colspan="3">验证人签字：　年　月　日</td></tr>
</table>

附表 10-4 涉密单位季度保密自查记录表示例

涉密单位季度保密自查记录表

单位		季度	年第　　季度
自查记录			
教育培训	1. 本季度组织保密教育培训____次，共____学时		
	2. 保密教育培训记录（○是　○否）完整、翔实，包括：□签到表 □培训内容 □其他：______________		
涉密人员管理	3. 本单位共有涉密人员____人		
	4. 本季度新增涉密人员____人，（○是　○否）按要求进行资格审查、岗前教育、涉密岗位和涉密等级审核		
	5. 本季度涉密人员密级调整____人，（○是　○否）按要求进行载体和设备的清退、变更		
	6. 本季度涉密人员脱密____人，（○是　○否）按要求进行载体和设备清退、明确脱密期管理接收单位及要求		
	7. 尚有在脱密期内的人员____人，本季度对____人进行了脱密期回访，（○是　○否）发现不符合脱密期管理要求的现象		
	8. 本季度申请出国境人员____人，（○是　○否）进行了审查审批和保密提醒		
	9. 本季度出国境人员返回____人，对____人进行了回访，（○是　○否）按时收回因私出国境证件并上交		
载体管理	10. 本季度制作涉密载体____份，收到外来涉密载体____份，送出涉密载体____份，销毁涉密载体____份		
	11. 制作、收发、传递、销毁涉密载体（○是　○否）按规定履行相应的审批、登记、受控手续		
	12. 涉密载体存放（○是　○否）符合要求		
	13. 涉密载体台账（○是　○否）完整、准确		
信息设备和存储设备	14. 本单位共有涉密信息设备____台、存储设备____个，非涉密信息设备____台、存储设备____个		
	15. 本季度新增信息设备____台、存储设备____个，变更信息设备____台、存储设备____个，报废信息设备____台、存储设备____个，销毁信息设备____台、存储设备____个，维修信息设备____台、存储设备____个		

续表

信息设备和存储设备	16. 信息设备和存储设备台账(○是　○否)及时更新,内容(○是　○否)完整、准确
	17. 本季度累计中转涉密信息____次、非涉密信息____次,(○是　○否)履行相应的审批、登记手续
	18. 本季度累计输出涉密信息____次、非涉密信息____次,(○是　○否)履行相应的审批、登记和内容审查手续
涉密场所	19. 本季度涉密场所(○是　○否)发生变化,界定(○是　○否)准确,责任人(○是　○否)明确,防范措施(○是　○否)到位
	20. 保密要害部门、部位(○是　○否)按要求进行月度自查
涉外交流	21. 在对外交流、合作和谈判等活动中(○是　○否)采取相应保密措施,对有关人员进行保密提醒
	22. 在对外交流、合作和谈判内容(○是　○否)经过审查
	23. 对外提供资料和物品(○是　○否)履行了保密审查、审批手续
涉密会议管理	24. 本季度主办(承办)涉密会议____场,其中重要涉密会议____场,场所和会议过程管理等(○是　○否)符合要求,重要涉密会议(○是　○否)到保密办备案
	25. 本季度携带涉密载体和涉密设备外出参加涉密会议____场
	26. 涉密会议使用的信息设备和存储设备(○是　○否)经过审批等级并符合保密管理要求
	27. 涉密会议载体发放、清退和销毁管理(○是　○否)经过审批等级并符合保密管理要求
宣传报道	28. 本季度对外报道、材料送审、发表论文(○是　○否)经过保密审查,共____次
	29. 本季信息发布(○是　○否)进行了保密审查审批,共____次
监督检查	本季度单位保密管理体系(○是　○否)发生了变化,(○是　○否)及时备案
	本季度对____名涉密人员进行了检查(填写相应的检查记录表,应确保全年覆盖本单位所有涉密人员),单位保密负责人/主管保密工作领导带队检查____次(请另附检查记录、简报等)
	对本季度保密检查中发现的问题(○是　○否)有效落实整改
存在问题及整改建议	
检查人/保密管理员签字： 年　月　日	

单位保密领导小组意见	负责人签字： 年　月　日	整改确认	验证人签字： 年　月　日

附表 10-5　泄密事件报告登记表示例

泄密事件报告登记表

<table>
<tr><td rowspan="7">事件基本情况</td><td>单　　位</td><td colspan="3"></td></tr>
<tr><td>当事人姓名</td><td></td><td>当事人职务</td><td></td></tr>
<tr><td>发生时间</td><td></td><td>发生地点</td><td></td></tr>
<tr><td>泄密方式</td><td></td><td>泄密密级</td><td></td></tr>
<tr><td>载体形式</td><td></td><td>泄密数量</td><td></td></tr>
<tr><td>泄密内容</td><td colspan="3"></td></tr>
<tr><td>发生经过</td><td colspan="3"></td></tr>
<tr><td rowspan="3">发现情况</td><td>发现时间</td><td></td><td>发现地点</td><td></td></tr>
<tr><td>发现人姓名</td><td></td><td>发现人单位</td><td></td></tr>
<tr><td>发现经过</td><td></td><td></td><td></td></tr>
<tr><td colspan="2">造成或可能造成的危害</td><td colspan="3"></td></tr>
<tr><td colspan="2">已进行或拟进行的查处工作情况</td><td colspan="3"></td></tr>
<tr><td colspan="2">已采取或拟采取的补救措施</td><td colspan="3"></td></tr>
</table>

填报人：　　　　　　　　单位领导(盖章)：　　　　　　　　年　　月　　日

附表 10-6　院系部处负责人保密工作年度考核记录表示例

院系部处负责人保密工作※※年度考核记录表

单位		负责人		职务	

序号	检　查　内　容	检查结果
1	是否参加党和国家关于保密工作的法律法规、方针政策的要求学习	□是　□否
2	是否熟悉武器装备科研生产单位保密资格标准	□是　□否
3	是否熟悉学校保密规章制度	□是　□否
4	是否清楚保密工作职责	□是　□否
5	是否对本单位开展保密工作提供条件保障	□是　□否
6	是否掌握业务工作中的重要涉密事项	□是　□否
7	是否知悉本部门涉密事项的密级、数量、人员的涉密等级等基本情况	□是　□否
8	是否积极落实学校部署的保密工作	□是　□否
9	是否每季度安排保密教育	□是　□否
10	是否每季度对保密措施落实情况进行检查，并对检查出的问题进行监督落实整改	□是　□否
11	是否关心专兼职保密工作人员	□是　□否
保密办意见	负责人签字（盖章）：　　年　月　日	

附表 10-7　＊＊大学所属单位年度保密工作考核表示例

＊＊大学所属单位＊＊年度保密工作考核表

单位：

序号	考核内容	分值	落实情况	得分
一	保密工作领导责任制落实情况	14 分		
1	对保密工作部署和落实提出明确要求，听取保密工作情况汇报并解决相关问题，将履行保密工作责任制情况纳入年度考评和考核内容，为保密工作开展提供人力、物力、财力等条件保障	4 分		
2	坚持保密工作领导小组议事制度，研究部署本单位保密工作并对落实情况组织检查，及时组织查处违规行为	3 分		
3	分管业务工作负责人对分管业务工作范围内的保密工作部署和落实提出明确要求，对落实情况进行督促检查，支持保密工作机构和人员开展工作	3 分		
4	掌握本部门保密工作情况，对涉密人员进行保密教育和管理，定期开展保密自查和季度检查，及时整改存在的问题	4 分		
二	保密制度建设情况	6 分		
5	结合单位实际建立健全各项保密制度和工作流程	3 分		
6	工作流程具有可操作性，责任追究和奖惩措施明确具体	2 分		
7	根据情况变化(学校的制度修订)及时修订完善相关保密制度或工作流程	1 分		
三	保密宣传教育培训情况	4 分		
8	对本单位保密宣传教育工作作出安排并组织落实	2 分		
9	及时传达学习保密工作文件和法规制度	1 分		
10	组织涉密人员保密知识技能培训，或者按要求参加学校组织的培训	1 分		
四	涉密人员管理情况	8 分		

续表

序号	考 核 内 容	分值	落实情况	得分
11	准确界定涉密岗位和涉密人员的涉密等级	1分		
12	涉密人员上岗前，进行审查和培训，使其了解相关保密法规制度。掌握相关保密知识技能，并组织签订保密承诺书	2分		
13	涉密人员在岗期间，所在部门督促其熟悉相关保密事项范围，履行本岗位保密职责，定期进行自查并及时整改存在的问题，并按照有关规定对涉密人员因私出国(境)等事项履行审批手续	3分		
14	涉密人员离岗前，按照有关规定监督其清退涉密载体，确定脱密期管理措施	2分		
五	国家秘密确定、变更和解除情况	6分		
15	明确本单位项目负责人承办定密事项及单位保密负责人审核权限	2分		
16	依法确定并标明国家秘密事项密级和保密期限	2分		
17	不将依法应当公开的事项确定为国家秘密	1分		
18	根据情况变化及时变更和解除国家秘密事项密级	1分		
六	国家秘密载体管理情况	8分		
19	国家秘密载体制作、收发、传递、复制、使用、保存、维修、销毁等符合保密管理规定	4分		
20	密品的研制、试验、使用、运输、保管、维修、销毁等符合保密管理规定	2分		
21	根据工作需要确定国家秘密事项的知悉范围，对知悉机密级以上国家秘密的人员作出书面登记	2分		
七	信息设备保密管理情况	20分		
22	涉密计算机采取符合国家保密标准的身份鉴别、访问授权、违规外联监控、病毒查杀、移动存储介质管控等安全保密措施，不安装使用具有无线功能的模块和外围设备	5分		
23	保持保密技术防护设施设备的防护性能	5分		

续表

序号	考 核 内 容	分值	落实情况	得分
24	建立健全计算机和移动存储介质登记台账，涉密计算机和移动存储介质粘贴密级标识，明确责任人、设备编号等	5分		
25	使用打印机、复印机、传真机等办公自动化设备符合保密管理规定	3分		
26	使用手机符合保密管理规定	2分		
八	涉密场所及保密要害部门、部位管理情况	4分		
27	按照有关规定对保密要害部门、部位采取人防、物防、技防等防护措施	2分		
28	落实禁止无关人员进入涉密场所和保密要害部门、部位的规定	2分		
九	涉密会议、活动管理情况	4分		
29	涉密会议、活动使用符合保密要求的场所、设施、设备	1分		
30	主办涉密会议或活动指定专人负责保密管理工作，落实各项保密措施。重要涉密会议成活动制定保密方案并报学校保密办备案	1分		
31	对提供涉密服务的外协单位进行保密审查，提出保密要求，签订保密协议	2分		
十	涉外工作保密管理情况	5分		
32	对外交流、合作等活动采取相应保密措施，对有关人员进行保密提醒	1分		
33	对外提供文件、资料和物品按规定经过保密审查审批，涉及国家秘密的应与外方签订保密协议	2分		
34	出国(境)团组指定专人负责保密工作，进行行前保密教育，落实各项保密措施	2分		
十一	宣传报道和信息公开保密审查情况	6分		
35	对外宣传报道履行保密审查审批程序	2分		
36	申报专利、成果、报奖等材料送审履行保密审查审批程序	2分		

续表

序号	考 核 内 容	分值	落实情况	得分
37	落实了网站信息发布登记制度	2 分		
十二	保密检查及违规行为处理情况	5 分		
38	对本单位保密检查工作制订计划并组织落实	2 分		
39	对保密检查中发现的违规行为及时组织整改	1 分		
40	对违规行为责任人员进行处理	2 分		
十三	保密工作领导小组职能设置、管理人员配备及经费保障情况	7 分		
41	保密工作领导小组组织健全，职责明确	3 分		
42	按规定指定专人负责保密工作	3 分		
43	保密工作所需经费有保障	1 分		
十四	保密工作记录和材料	3 分		
44	建立保密工作记录，各项保密工作落实情况材料翔实完整	3 分		
十五	否决项		扣分方法	扣分
45	涉密计算机接入互联网及其他公共信息网络		发现 1 起扣 5 分	
46	非涉密计算机存储、处理和传输国家秘密信息		发现 1 起扣 5 分	
47	涉密信息设备与非涉密信息设备之间交叉使用移动存储介质		发现 1 起扣 5 分	
48	发生泄密事件		直接评定为不符合要求	
总得分		考评结果	□符合要求 90 分以上 □基本符合要求 80～89 分 □不符合要求 80 分以下	

说明：如果实际工作无相应内容，不扣分。

附表 10-8　涉密人员年度保密考核表示例

涉密人员 ＊ ＊ 年度保密考核表

单　位		姓　名	
涉密岗位		涉密等级	
考 核 内 容			
保密责任	1. 是否按照保密责任书要求履行相应保密职责　是□　否□ 2. 未完成事项说明：		
保密教育	本年度完成保密教育______学时，其中 1. 参加学校保密教育____学时 2. 参加所在单位（含课题组）保密教育______学时 3. 参加校外保密教育____学时（组织单位：　　） 4. 其他：____学时		
保密检查	1. 本年度接受上级单位、学校、院系保密检查____次 2. 是否发现违反保密规章制度的情况　是□　否□ 3. 检查发现的主要问题是否及时采取整改措施　是□　否□		
出国（境）情况	1. 本年度因公出国（境）__次，是否签订因公出国保密承诺书　是□　否□ 2. 本年度因私出国（境）__次，是否签订因私出国（境）保密审查表　是□　否□		
失泄密事件	本年度是否发生失泄密事件　是□　否□		
本年度履行保密责任简述	本人签字：　年　月　日		
课题组意见	（课题组涉密人员） 1. 上述情况是否属实　是□　否□ 2. 履行保密职责情况　符合要求□　基本符合要求□　不符合要求□ 负责人签字：　年　月　日		
单位考核意见	本年度履行保密职责情况： 考核合格□　考核不合格□ 主管领导签字：　年　月　日		

附表 10-9　保密工作先进集体推荐表示例

保密工作先进集体推荐表

<table>
<tr><td>集体名称</td><td colspan="2"></td><td>所在单位</td><td colspan="2"></td></tr>
<tr><td>保密
责任人</td><td></td><td>涉密人
员数量</td><td></td><td>涉密计算
机数量</td><td></td></tr>
<tr><td>先进事迹</td><td colspan="5"></td></tr>
<tr><td>推荐
单位
意见</td><td colspan="5">（公　　章）
单位负责人：　　　　年　　月　　日</td></tr>
<tr><td>评审小组
意见</td><td colspan="5">组　长：
年　　月　　日</td></tr>
</table>

附表 10-10　保密工作先进个人推荐表示例

保密工作先进个人推荐表（表头）

<table>
<tr><td>姓　名</td><td></td><td>性别</td><td></td><td>工作单位</td><td></td></tr>
<tr><td>岗位名称</td><td colspan="5">□保密工作负责人　□项目负责人　□专兼职保密工作人员　□项目参与</td></tr>
</table>

附件 10-11　惩处情形示例一

对直接责任人依据违规行为进行保密惩处的情形

一、进行谈话提醒的行为

1. 在公共场所谈论国家秘密的；

2. 收发、传递涉密载体未履行登记、签收手续的；

3. 在涉密计算机上存储、处理个人信息等与工作无关资料的；

4. 将个人具有存储功能的存储介质和电子设备带入重要涉密场所的；

5. 制作、打印密件，无密级标识或擅自更改密级标识的；

6. 逃避或妨碍保密检查的。

二、教育备案的行为

1. 本年度谈话提醒两次及以上的；

2. 擅自在涉密计算机上安装与工作无关软件的；

3. 在无加密措施的通信工具（如固定电话/手机、无绳电话/无线对讲机等）谈论国家秘密的；

4. 未经批准，擅自复制秘密级文件、资料的；

5. 复制、下载、打印、扫描涉密文件，遮盖原密级标识的；

6. 涉密文件、涉密移动存储介质、涉密便携式计算机等涉密载体未按规定存放的；

7. 对发现问题拒不整改的。

三、通报批评和 200～1000 元经济处罚的行为

1. 本年度受教育备案两次及以上的；

2. 未经审批携带密品、密件外出的；

3. 擅自拍摄、录音、抄录、摘录涉密信息的；

4. 擅自将国（境）外人员带入指定范围以外场所的；

5. 擅自将无关人员带入涉密场所的；

6. 擅自变更涉密计算机用途、涉密性质和软、硬件配置的；

7. 未经批准，对涉密计算机进行格式化处理或者重装操作系统的；

8. 未采取有效防范措施（如查毒和恶意代码查杀等），直接将数据拷贝到涉密信息设备或涉密信息系统中的；

9. 拒绝在涉密计算机内安装终端防护及其他安全管理软件，或新购设备及重装系统后一周内未按要求申报安装终端防护及其他安全管理软件的；

10. 擅自报废处理有存储功能的涉密复印、传真、打印设备及各类涉密信息载体的；

11. 遗失涉密载体或致使涉密载体不可控，但及时找回的；

12. 丢失门禁系统、计算机及涉密信息系统等身份鉴别设备不及时报告的；

13. 私自存留国家秘密或曾经处理、存储过国家秘密载体和设备的；

14. 利用职权指使他人违反保密规定，未造成严重后果的（造成严重后果的视同直接责任人追究责任）；

15. 涉密信息系统管理人员有下列行为之一的：

- 文档化安全策略不完整的，或文档化安全策略与信息系统实际安全策略严重不符的；
- 未按照规定周期对审计记录进行审查或分析，形成文档化审计报告的；
- 未按照规定周期对涉密信息系统风险自评估，形成文档化分析报告的；
- 其他不按保密规定及相关标准履行职责的行为。

16. 其他违反保密规定、未造成后果的行为。

四、给予责任人行政警告处分（是党员的并处相应的党纪处分）和1000～3000 元经济处罚的行为

1. 擅自将计算机接入涉密信息系统的；

2. 涉密计算机未拆除或禁用红外和无线传输设备（如无线网卡、无线鼠标、无线键盘、红外接口等）的；

3. 泄露、印证泄露或遗失秘密级信息、载体造成后果的；

4. 在非涉密传真机上传输秘密级信息的；

5. 未经审批，擅自复制机密级文件、资料的；

6. 未经审查，擅自对外提供秘密级载体或信息的；

7. 非法获取、使用、更改他人涉密信息系统身份信息（如口令等）的；

8. 擅自将涉密计算机及存储设备、涉密电子设备等送到非指定部门维修的；

9. 其他违反保密规定的行为。

五、给予责任人行政记过处分（是党员的并处相应的党纪处分）和3000～5000元经济处罚的行为

1. 对特殊渠道获取的设备、资料未采取保密措施或措施不当的；

2. 未按保密规定使用绝密级计算机的；

3. 在非涉密传真机上传输机密级信息的；

4. 未经审查，擅自对外提供机密级载体或信息的；

5. 泄露、印证泄露或遗失秘密级信息、载体（含曾经存储过秘密级信息的一般载体），不及时报告和隐瞒不报的（口头报告应在4小时之内，书面报告应在12小时之内）；

6. 泄露、印证泄露或遗失机密级信息、载体造成后果的；

7. 其他严重违反保密规定的行为。

六、给予责任人行政记大过处分（是党员的并处相应的党纪处分）和5000～10 000元经济处罚的行为

1. 泄露、印证泄露或遗失机密级载体（含曾经存储过机密级信息的一般载体）不及时报告或隐瞒不报（口头报告应在4小时之内，书面报告应在12小时之内）和不及时采取补救措施的；

2. 使用黑客攻击、探测扫描程序等方式在涉密网络上收集、制作、传播计算机病毒等破坏性行为；

3. 将涉密存储介质在互联网计算机上使用的；

4. 擅自复制绝密级文件、资料的；

5. 其他严重违反保密规定的行为。

七、给予责任人降职、撤职处分(是党员的并处相应的党纪处分)和10 000～20 000元经济处罚的行为

1. 泄露国家秘密构成犯罪,被依法不起诉或者免于刑事处罚的;

2. 故意或过失泄露国家秘密不够立案标准,但给学校造成不良影响的;

3. 在互联网计算机上处理或存储、传递涉密信息的;

4. 将涉密信息系统(含涉密单机)直接或间接联入互联网或其他网络的(含通过多功能一体机、手机等与公共网络连接的);

5. 泄露绝密级国家秘密或遗失绝密级载体的;

6. 违反保密规定造成机要密码电话、密码机或密钥等通信加密设备丢失但未造成后果的;

7. 其他严重违反保密规定的行为。

八、给予责任人开除处分(或解除劳动合同,是党员的并处相应的党纪处分)的行为

1. 过失泄露绝密级信息后隐瞒不报或不如实提供情况,妨碍有关部门查处的;

2. 泄露机密级信息5项及以上,或者绝密级信息3项及以上的;

3. 涉密人员携带涉密载体擅自离职或离境,对国家安全和利益构成严重威胁的;

4. 因违反保密规定受到刑事处罚的;

5. 其他严重违反保密规定的行为。

以牟取私利为目的泄露国家秘密的,加重处罚,触及法律的移交司法机关处理。

附件 10-12　惩处情形示例二

对直接责任人依据扣分情况进行保密惩处的情形

按照武器装备科研生产单位保密资格标准和评分标准：

一、一年内累计扣分 3 分(含)至 8 分的

由所在单位对直接责任人进行约谈，停发三个月保密补贴。

二、一年内累计扣分 8 分(含)至 11 分的

由所在单位对直接责任人进行约谈，在单位内部进行通报，停发六个月保密补贴。

三、发现中止项和重点项，或者一年内违规扣分 12 分以上的

由保密管理办公室对直接责任人进行约谈，责成作出书面检查，在单位内部进行通报，停发一年保密补贴；

情节严重的，经保密委员会批准，通过在全校进行通报、取消本年度学校各级评优资格等方式追究责任；

涉及违法违规的，依法依规追究相关责任。

附件 10-13　惩处情形示例三

对相关负责人保密问责的情形

一、直接责任人受到开除处分

给予责任部门主要负责人和分管保密工作负责人撤职、降级、记大过、记过、警告处分，并处经济处罚。

二、直接责任人受到记大过及降职、撤职处分

给予责任部门主要负责人和分管保密工作负责人警告处分或通报批评，并处以经济处罚。

三、直接责任人受到记过及以下行政处分

给予责任部门分管保密工作负责人通报批评。违法违规行为由责任单位自查发现，并积极采取措施补救，挽回或减轻损害的，可视情减轻或免于追究有关领导责任。

第十一章　保密条件保障

保密条件保障是学校开展保密工作的基本要求和必要条件，主要涉及保密工作经费和保密工作档案。为了更好地促进保密责任的落实，提高保密管理的精细化水平和保密管理工作效率，推进保密管理信息化已成为大势所趋。

一、保密工作经费

保密工作经费是学校用于开展保密工作的费用，分为保密管理工作经费和专项保密工作经费。保密管理工作经费用于学校的日常保密管理工作；专项保密工作经费用于保密防护设施的建设和设备的配备等。

学校保密管理办公室所需的保密管理工作经费应当列入学校年度财务预算，其他各部门保密管理工作经费根据工作需要予以保障；各部门专项保密工作经费应当按照实际需要予以保障。

（一）保密管理工作经费

保密管理工作经费不是学校保密管理办公室的办公经费，应当主要用于开展保密教育培训、保密工作调研、咨询、宣传、项目评审、表彰奖励等工作所发生的费用以及保密专用小型设备的购置，如手机屏蔽柜、会议保密机等，不得用于人员工资以及办公设备购置、保密补贴等支出。

学校保密管理办公室所需的保密管理工作经费应当列入学校年度财

务预算，涉密人员每人每年度保密管理经费标准进行预算：①核心涉密人员每人每年度 300 元；②重要涉密人员每人每年度 200 元；③一般涉密人员每人每年度 100 元。

合计高于 50 万元的学校，以 50 万元为保证基数；低于 10 万元的以 10 万元为保证基数，不足部分按照工作需要增补。

例如，某一级保密资格高校涉密人员 1500 人，其中核心涉密人员 20 人，重要涉密人员 400 人，一般涉密人员 1080 人，那么该高校保密管理工作经费标准为：

$$20\times300+400\times200+1080\times100=194\ 000(\text{元})$$

则该高校纳入单位预算的保密管理工作经费不得少于 19.4 万元，不足部分按照工作需要增补。

再如，某二级保密资格高校涉密人员 500 人，其中重要涉密人员 100 人，一般涉密人员 400 人，那么该高校保密管理工作经费标准为：

$$100\times200+400\times100=60\ 000(\text{元})$$

此标准未达到 10 万元保证基数，按照要求，该校纳入单位预算的保密管理工作经费则不得少于 10 万元。

学校所属各单位的保密管理工作经费应当由各单位按需保证。

学校保密管理办公室及所属各单位的保密管理工作经费应当根据工作需要保证足额开支。

（二）专项保密工作经费

专项保密工作经费是专门用于解决日常保密工作经费顾及不到、解决不了的重大保密问题而设置的经费，如保密要害部门部位内外环境技术防护设施和设备的购置，计算机监控审计与身份识别系统的购置或升级、保密检查设备的购置、涉密网络的建设等。具体包括：

（1）保密防护设施的建设和设备的配备：如视频监控系统的配备或升级、门禁系统的配备或升级、防盗报警系统的配备或升级、保密会议室屏蔽措施升级等。

（2）大批量采购保密专用设备：如电子密码铁皮柜、保险柜、碎纸机、光盘粉碎机、会议保密机等。

（3）涉密计算机安全防范经费。

（4）保密技术检测工具：如信息系统违规操作检查工具、非法外联检查工具等。

（5）涉密网络建设与互联网信息安全防范经费。

（6）其他开展的保密专项工作经费。

专项保密工作经费应由学校或使用单位予以充分保障。对新建项目，其安全保密防范设施应当与建设项目同步设计、同步预算、同步施工、同步验收；对技术改造项目，应当在技术改造经费中按需安排安全保密防范设施设备经费，确保达到安全保密标准。

二、保密工作档案

保密工作档案是保密工作开展情况的记载，是保密工作开展的佐证。档案内容应当完整真实，能够反映单位保密工作开展实际情况。学校保密管理办公室和相关职能部门、涉密院系应当按照职责分工，分别建立并妥善保存保密工作档案。学校及所属各单位保密工作档案保存期限一般不少于 3 年，通常为 5 年（与保密资格认定周期一致）。涉密载体移交记录等要求长期保存的除外。

（一）校级保密工作档案

校级保密工作档案是指学校保密管理办公室和相关职能部门按照归口管理的原则履行相关保密监督管理职责的工作记载。主要包括：

1．领导保密责任制

包括学校党政主要领导（校长、党委书记）、分管保密工作领导及各个业务领导针对保密工作的批示，在党委常委会、党委扩大会、校务会、中层干部会等各种会议上有关保密工作的讲话，校领导研究解决保密工作机构

建设、保密条件保障等保密工作重大问题或研究部署年度保密工作要点或协调解决保密工作中的重点难点问题的会议记录、述职材料等，听取保密工作汇报、监督检查保密工作落实情况的记录，以及各级领导的保密责任书等。

2. 保密组织机构

包含保密委员会与保密工作机构的工作档案。

保密委员会：主要包括学校保密委员会组成及调整情况、职责分工及开展工作的记录（包含保密委员会例会记录，研究解决重要问题的记录，保密委员会成员年底述职述密报告等）；

保密工作机构：主要包括学校保密机构设置及职能的文件，专职保密工作人员数量、分工及知识技能等证明材料，保密管理办公室履行职责的记录（包含年度保密工作计划、保密工作记录及保密工作总结等）。

3. 保密制度

一般包括校级保密规章制度汇编、针对重大涉密工程或者项目制定的专项保密制度以及各基层单位的二级保密制度汇总。

校级保密规章制度汇编包括学校保密工作规定与标准规定的各项基本制度，以及面向学校各涉密单位的业务制度（如涉密项目保密管理办法及研究生学位论文保密管理办法等），还应当提供校级保密规章制度通过校务会或保密委员会审议的记录。

4. 定密管理

包括定密授权文件（上级业务主管部门对学校进行授权以及学校法定定密责任人对指定定密责任人进行授权）、定密责任人资格认定证明材料、定密程序及依据文件、《定密细目》、学校组织开展国家秘密事项确定、变更及解除的工作记录等。

5. 涉密人员管理

包括涉密人员上岗、在岗、离岗等动态管理档案，涉密人员台账，在岗管理主要包括保密教育培训记录、保密工作考核记录、因私出境管理记录与保密补贴发放记录等。

6. 涉密载体管理

包括载体制作、收发、传递、借阅、使用、复制、保存、销毁的闭环管理记

录，以及载体受控章管理记录、载体集中销毁记录、载体统计记录以及保密本管理记录等。

7. 密品管理

主要包括密品台账，外场试验长途运输安全保密方案以及销毁记录等。

8. 保密要害部门、部位管理

包括学校保密要害部门、部位台账，部门、部位确定和变更情况，保密防护措施建设及验收情况，工勤服务人员保密管理措施，新建及改建工程保密防护措施与工程同步建设情况，以及具体部门、部位的管理办法等文字记录。

9. 信息系统、信息设备和存储设备管理

涉密信息系统通过测评记录，信息化管理部门组织制定的信息安全保密管理体系文件以及运行维护机构制定的运行维护工作制度和操作规程，"三员"或涉密计算机安全保密管理员配备情况及资格认定证明材料；涉密人员使用的信息系统、信息设备和存储设备（含涉密、不联网及联网三类）台账，涉密信息系统、信息设备和存储设备密级确定与变更、安全防护与维护、携带外出、维修、报废等全寿命周期管理等记录。

10. 新闻宣传管理

主要包括涉及武器装备科研生产事项的宣传报道、展览、发表著作和论文等的保密审查记录以及涉及武器装备科研生产事项的参观、采访审批记录等。

11. 涉密会议管理

主要包括涉密会议审批表、会议签到及涉密载体发放记录、会议保密检查记录等。

12. 外场试验管理

主要包括外场试验保密工作方案，参加人员保密审查提醒记录，密品押运记录，外场试验现场密品密件等保密管理记录，保密检查记录以及试验结束后的保密总结记录等。

13. 协作配套管理

主要包括涉密协作配套项目及协作配套单位保密资格情况一览表，协

作配套项目合同文本(含保密条款)、保密协议书以及协作配套单位的保密资格证书,项目执行过程中保密监督检查记录等。

校外分包涉密任务涉及保密要害部门部位技术防护措施建设、国家秘密载体印刷、军工涉密业务咨询服务以及涉密信息系统集成业务的,还应当提供协作配套单位相应的涉密安防监控资质、国家秘密载体印制资质、军工涉密业务咨询服务资质以及涉密信息系统集成资质,以及与协作配套单位签订的保密协议等。

14. 涉外管理

主要包括涉密人员对外合作、交流、谈判等外事活动保密方案、保密审查及保密提醒记录,涉密单位接待境外来访的保密审查记录及安全防范措施等。

15. 保密检查

主要包括年度保密检查计划,综合保密检查、专项保密检查记录以及问题整改记录,各部门自查及整改情况报告,学校保密监督检查汇总分析报告(含保密风险分析)以及接受上级部门检查的记录等。

16. 泄密事件查处

学校发生的泄密事件报告与查处记录等。

17. 考核与奖惩

主要包括对各涉密单位、涉密人员组织年度考核的记录,各单位考核情况与绩效挂钩的记录,组织保密先进评选及奖励的记录,以及对违反保密规章制度或者不履行保密责任者进行追究的记录等。

18. 保密工作经费

主要包括保密管理工作经费纳入学校年度财务预算的记录,要求其额度符合要求,支出项目、额度符合规定;还包括专项保密工作经费按需批复的记录和各种支出记录等。

19. 保密工作档案

按照标准要求档案分类立卷,项目齐全,内容充实,记录清楚,便于检索。

（二）部门保密工作档案

部门保密工作档案是学校所属各涉密单位保密体系运行的记录，主要包括本单位涉密项目、涉密人员、涉密设备及涉密人员使用的非涉密设备台账，涉密设备使用记录（如打印、刻录审批、信息交换登记等），涉密载体制作、收发、复印、传递、销毁等闭环管理记录，涉密人员岗前、在岗、离岗记录，涉密场所进出记录以及单位内部保密培训、检查记录等。

三、保密管理信息系统

当前高校保密工作日益科学化、体系化，对人员管理、载体管理、信息设备管理以及监督检查等各方面都提出了更高的要求，相关的管理工作也日趋精细化、复杂化，工作量日益增大，为了进一步提高保密管理水平，建设保密管理信息系统的需求日益凸显。

（一）保密管理信息系统的优势

建设保密管理信息系统既有利于各类保密管理信息的更新与共享，也便于信息的利用，还有利于推进各类保密审查审批的电子化。概括起来，保密管理信息系统主要有以下四方面优势：

1. 实现数据信息的及时更新和相互关联

涉密项目、涉密事项、涉密人员、涉密设备、涉密场所、涉密载体等保密管理台账是各高校开展保密工作的抓手，通过建设保密管理信息系统，一方面可以实现各种台账在线（对建立涉密信息系统的单位）或定期（对单机版运行的保密管理信息系统）更新、数据共享，并能根据设定条件方便高效地进行各类查询统计；另一方面还可以实现台账信息之间的相互关联，如通过涉密项目获取其包含的涉密事项信息，进而获取知悉范围人员信息、使用的涉密设备与工作的涉密场所等信息，还可以包含涉密项目研制过程中产生的涉密载体信息；而通过查询涉密人员，也可以方便地获取其承担

或参加的涉密项目、知悉的涉密事项、使用的涉密设备、工作所在的涉密场所、产生涉密载体等信息，进而从涉密人员、设备、载体等独立的保密要素全生命周期管理跃升为整个保密体系的全生命周期管理。

2. 简化保密审批流程，方便实现闭环管理

在日常涉密科研生产过程中，大量保密工作开展都要求履行相应的审批程序，各类保密审批流程多达几十个，甚至上百个。以涉密文件管理为例，涉密文件涉及打印、复印、利用、传递、销毁等各个环节，都要求履行相应的审批、登记手续，形成大量的纸质审批记录，一定程度上影响了工作效率，也容易出现审批不及时、登记信息不全、审批信息与登记信息不一致。同时，在人工管理模式下，各个管理环节形成档案记录彼此相互孤立、无法自动关联，追溯涉密载体的全生命周期管理存在很大难度。建立涉密信息系统，利用信息化管理手段，可以将涉密文件的产生、使用到传递、销毁等各个过程的审批在信息系统中实现，查询某一份涉密文件，其流转情况便可以在一张表格中体现，真正做到涉密载体可控、可管、可追溯、可闭环。

3. 提升保密检查效率，便于日常保密监管

在人工管理、纸质审批的情况下，学校开展保密检查往往需要耗费大量的精力进行资料审查，如果采用保密管理信息系统的方式，现场检查中可以利用各涉密单位的保密管理信息系统，结合现场工作情况，对各项工作进行审查，便于检查组迅速掌握被检查单位情况，提高检查深度与效率。而学校各涉密单位与学校保密管理办公室在线更新或定期汇总保密管理数据，也有利于各归口管理部门及时掌握各涉密单位的保密管理情况。

4. 便于保密管理信息的统计查询、汇总分析，为管理决策提供支持

建立保密管理信息系统，一是便于保密管理动态信息的统计，如历年产生的涉密文件、涉密设备、涉密科研项目、每个涉密人员的变动、出国(境)情况等信息；二是可实现保密管理档案电子化管理，提供目录管理、原件扫描、报表打印等功能；三是便于对学校保密管理数据整理、分析、挖掘，如对历次保密检查发现问题的整理分析，对历年来涉密项目负责人变动情况进行分析等，为学校进一步加强保密管理工作提供决策支持。

（二）需求分析

保密管理信息系统可以包含以下几方面管理内容：

1. 涉密项目、涉密人员和信息设备台账化管理

保密管理信息系统首先应包括涉密项目、涉密事项、涉密人员、信息设备、存储介质、涉密载体等台账，并相互关联，能根据条件进行各类查询统计。

2. 日常保密管理审批流程化和闭环管理

保密管理信息系统应涵盖涉密人员、信息设备、涉密载体、涉密会议、自查自评等相关活动所有的申请和审批流程化、规范化，全程可查询、可追溯、可控制，流程审批后的处理人、处理时间、处理方式均可纳入系统，实现闭环管理。

3. 涉密人员、涉密设备、涉密载体实现全生命周期管理

保密管理信息系统应记录涉密人员入密管理、在岗管理（含保密教育、出国（境）、保密补贴、密级调整、保密考核）、脱密等管理记录；涉密设备申请、使用（含安全策略的制定及下发）、维护维修、更新、封存、报废等全过程管理记录；涉密载体申请、审批、制作、保存、借阅、归还、传递、销毁等全过程管理记录。在此基础上，同时能够记录接触涉密载体的人员、各时间段的相关责任人等关联信息，实现纸质涉密载体条码化管理。

4. 保密工作档案电子化管理

保密管理信息系统应提供目录管理、原件扫描、报表打印、文件（保密）柜管理、保密期限到期提醒等功能。

5. 实现与现有涉密信息系统功能集成

对已建立涉密信息系统的高校，通过与之功能集成，可进一步拓展保密管理信息系统的功能。如按照计划自动对涉密计算机及其他涉密设备进行检查，能够结合已有的保密监管系统实现时时监控；对发现的问题与安全保密事件从发生到中间处理以及最终结果等环节进行全程动态的跟踪管理，实现保密检查自动化和常态化；通过年度的综合，并结合自查自评，将保密工作与个人和部门的绩效考核进行有效的关联。

（三）功能设计

保密管理信息系统功能结构图参见图 11-1，可具备以下基本功能。

1. 涉密项目管理

包括涉密项目台账、执行状态、涉密事项台账、外协项目台账、外协单位保密资格信息与保密监督检查管理等，建立校级、院系部门级和个人的三级台账信息库。

2. 涉密人员管理

包括涉密人员台账、基本信息、涉密等级、因私出国境、脱密期和对外科技交流等审批流程与信息管理，实现涉密人员规范化管理与动态管理。

3. 涉密设备管理

包括信息设备及存储设备、通信及办公自动化设备等台账化管理，实现借用、审批、维修维护与报废等全生命周期的管理，建立校级、院系部门级和个人的三级台账信息库。

4. 涉密载体管理

实现涉密载体申请、审批、制作、借阅、保存、传递和销毁的全生命周期管理。

5. 保密档案管理

实现校级保密档案管理、机要室档案管理以及部门内部保密档案管理的分级管理，实现保密档案管理的信息化和电子化。

6. 保密检查管理

实现保密自查提醒和问题报告，实现学校级、部门级的保密检查提醒、计划制订、问题汇总与处置等功能。

7. 日常工作管理

包括保密组织机构管理、保密制度管理、要害部门部位管理、保密会议管理、涉外活动管理和对外交流（包括宣传、报道、展览、论文等）管理等日常保密工作的管理。

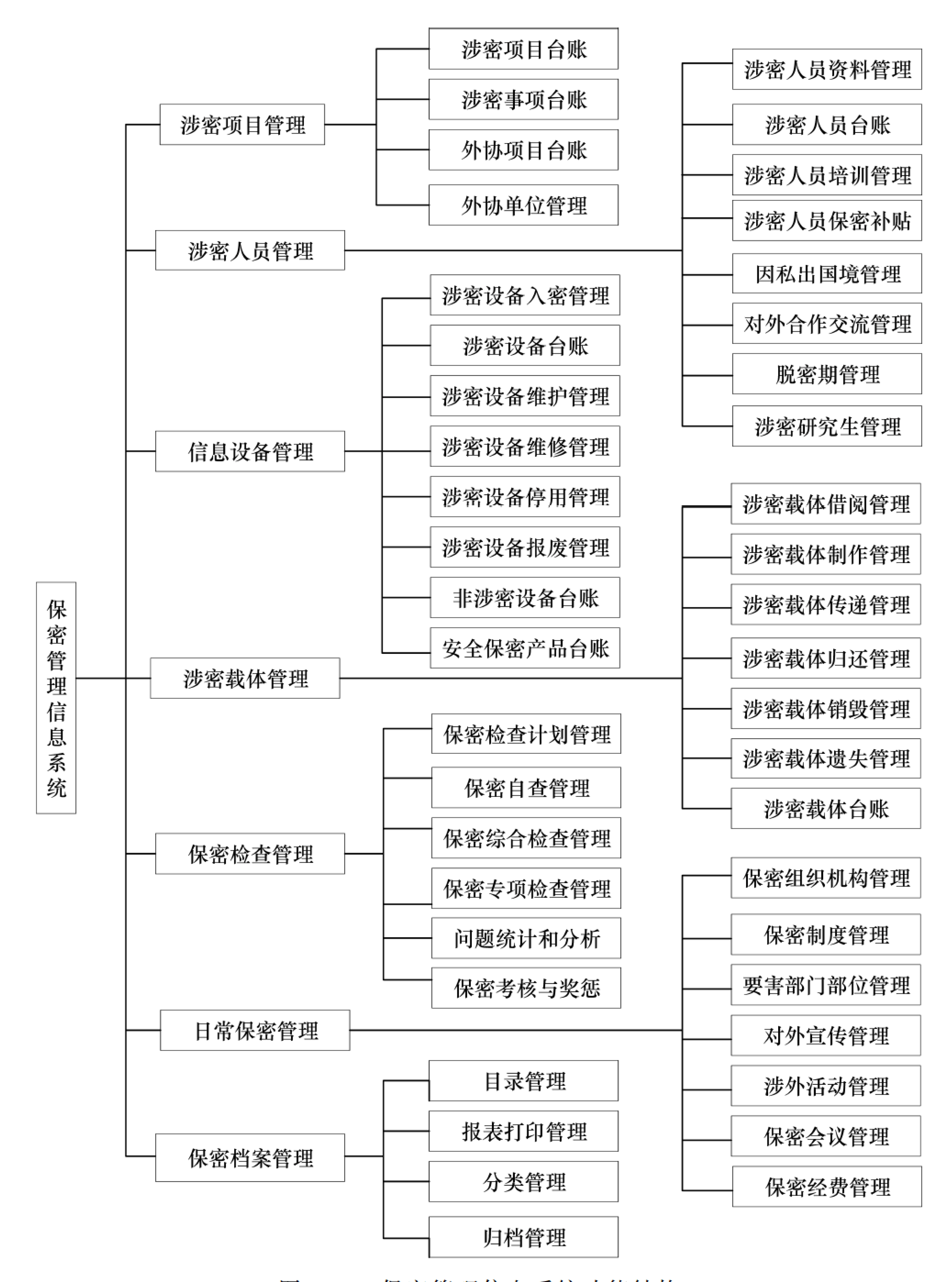


图 11-1　保密管理信息系统功能结构

（四）建设注意事项

建设保密管理信息系统，是保密管理更加规范、科学的一个抓手，也是保密工作与时俱进的体现，在推行保密信息化管理的过程中，为了使保密管理信息系统更加有效地运行，应当注意以下方面：

1. 综合分析本单位保密、信息化管理情况

由于保密管理信息系统中包含有项目、密点、设备、人员等大量信息，这些信息虽然可以先经过脱密处理，但部署在非涉密计算机上仍存在较大的隐患，建议在涉密环境下部署保密管理信息系统。目前，建设保密管理信息系统主要基于两种模式：基于单机版的保密管理信息系统与基于网络版的保密管理信息系统，前者适用于尚未建立涉密信息系统的单位，后者适用于已建立涉密信息系统的单位。同时，后者运行也分为两种情况，一是建立与单位 OA 系统相结合，将审批流程固化在 OA 系统中；二是按照军工保密资格认定标准保密责任、保密组织机构、保密制度、保密监督管理、保密条件保障五大项内容建立独立的保密管理信息系统，具体采取的模式必须结合本单位保密、信息化管理的实际情况统筹考虑。有些单位的应用系统运行如果已经比较稳定，基本可以满足日常办公需要，则可采取第一种方式，将保密管理的内容融入已有的信息化系统中，避免单位内多个信息管理系统运行造成的数据流冲突、资源浪费；有些单位如果目前还没有建立 OA 系统或者现有的应用系统较少，可采取第二种模式，对现有的保密档案、资料进行全面整理，使保密管理流程更加清晰。

2. 系统规划、逐步推进

保密管理信息系统应当按照涉密信息系统的要求进行规划和设计，架构上要做好三元的权限划分，功能上在需求分析的基础上进行系统设计并逐步推进。如单机版的保密管理信息系统可先实现各种信息台账的定期更新交互及信息关联的功能，并采取模块化设计，为其他功能拓展预留空间，同时考虑单机版向网络版拓展的未来需求。对网络版的保密管理信息系统，要充分考虑单位目前已有的信息化系统，确保综合利用现有信息化

管理资源,确保实现系统接口顺利对接,防止出现数据重复利用、审批重复流转、资源无端浪费的现象。保密管理信息系统可以由单位自行开发或找有相应资质的公司开发。

3. 全面整理单位已有保密管理档案和资料

在明确保密管理信息系统的基本模式、基本框架,确保接口融合的情况下,还应对单位目前的保密档案、资料进行全面整理,统一纳入保密管理系统,防止出现部分内容游离于管理信息系统之外的现象,更好地实现保密信息化管理。

总的来说,建设保密管理信息系统是简化审批流程、强化保密管控、细化保密管理、有效开展审查、及时掌握数据、实现长效机制的必由之路。各高校在具体建设时需要结合本单位的实际情况进行全面考虑和全盘部署。同时,建立保密管理信息系统不是一蹴而就、一劳永逸的事情,需要不断加强日常的管理,实现与信息化管控相结合,更好地完善保密管理工作,形成规范、科学的保密管理体系。

主要参考文献

1.《中华人民共和国保守国家秘密法》(2010 年 4 月 29 日中华人民共和国主席令第 28 号公布)

2.《中华人民共和国保守国家秘密法实施条例》(2014 年 1 月 17 日中华人民共和国国务院令第 646 号公布)

3.《武器装备科研生产单位保密资格认定办法》(国保发〔2016〕15 号)

4.《武器装备科研生产单位保密资格标准和评分标准》(国保发〔2016〕43 号)

5.《中共中央保密委员会关于加强国防科技工业保密管理工作的意见》(中保发〔2001〕21 号)

6.《关于进一步加强涉密人员保密管理工作的意见》(国保发〔2015〕5 号)

7.《国务院、中央军委关于建立和完善军民结合、寓军于民武器装备科研生产体系的若干意见精神》(国发〔2010〕37 号)

8.《手机使用保密管理规定》(中共中央办公厅、国务院办公厅印发〔2014〕45 号)

9.《国家秘密载体销毁管理规定》(厅字〔2009〕18 号)

10.《国家秘密定密管理暂行规定》(国家保密局令 2014 年第 1 号发布)

11.《国家秘密设备、产品的保密规定》(国保发〔1992〕53 号)

12.《新闻出版保密规定》(国保发〔1992〕34 号)

13.《报告泄露国家秘密事件的规定》(国保发〔1999〕8 号)

14.《中共中央保密委员会办公室、国家保密局关于国家秘密载体保密管理规定》(厅字〔2000〕58 号)

15.《对外经济合作提供资料保密暂行规定》(国保发〔1993〕28 号)

16.《对外科技交流保密提醒制度》(国保发〔2002〕7 号)

17.《中共中央保密委员会办公室、国家保密局关于保密要害部门部位保密管理的规定》(厅字〔2005〕1 号)

18.《关于切实做好新形势下涉外保密工作的实施意见》[中保办(局)发〔2005〕6 号]

19.《涉及国家秘密的通信、办公自动化和计算机信息系统审批暂行办法》(中保办发

〔1998〕6 号）
20.《党政机关和涉密单位网络保密管理规定》（中共中央办公厅国务院办公厅印发〔2015〕15 号）
21.《涉及国家秘密的计算机信息系统集成资质管理办法》（国保发〔2013〕7 号）
22.《关于加强新技术产品使用保密管理的通知》（国保发〔2006〕3 号）
23.《涉及国家秘密信息系统分级保护管理办法》（国保发〔2005〕16 号）
24.《涉及国家秘密的信息系统审批管理规定》（国保发〔2007〕8 号）
25.《涉及国家秘密的载体销毁与信息消除安全保密要求》（BMB21—2007）
26.《国防科技工业涉密人员保密管理办法》（科工安密〔2016〕1388 号）
27.《国防科技工业安全防范系统技术要求》（科工安密〔2012〕967 号）
28.《关于禁止邮寄或非法携运国家秘密文件、资料和其他物品出境的规定》（国保发〔1994〕17 号）
29.《国防科技工业保密责任制规定》（科工安密〔2015〕1286 号）
30.《教育部、国家保密局关于加强高等学校保密管理工作的通知》（教办〔2009〕5 号）
31.《军工单位七类人员安全保密管理措施（试行）》（科工安密〔2010〕1021 号）
32.《军工涉密业务咨询服务安全保密监督管理办法（试行）》（科工安密〔2011〕356 号）
33.《军工涉密业务咨询服务安全保密监督管理办法（试行）》（科工安密〔2012〕105 号）
34.《国防科技工业安全保密八个集中管理》（科工安密〔2012〕736 号）
35.《国防科技工业离退休人员安全保密管理规定》（科工安密〔2012〕1473 号）
36.《关于加快吸纳优势民营企业进入武器装备科研生产和维修领域的措施意见》（装计〔2014〕809 号）
37.《国防科技工业国家秘密范围的规定》（科工安密〔2009〕1488 号）
38.《教育工作中国家秘密及其密级具体范围的规定》（教办〔2017〕3 号）
39. 国家军工保密资格认定办公室：《军工保密资格认定工作指导手册》，北京，金城出版社，2017.
40. 王桂芝等：《高校基层部门科技保密管理工作的几点体会》，载《科研管理》，2008(29).
41. 崔淑妮等：《建立高校保密长效管理机制的几点思考》，载《科研管理》，2010(31).
42. 崔淑妮等：《基于过程方法的涉密项目保密管理探究》，载《西南交通大学学报》，2011(12).
43. 李继红等：《高校国防科研定密工作初探》，载《科研管理》，2012(33).

44. 游庆章主编:《高校保密工作的理论与实践》,昆明,云南大学出版社,2009.
45. 李新荣:《高等院校科研管理研究》,北京,中国经济出版社,2008.
46. 封化民主编:《保密管理概论》,北京,金城出版社,2014.
47. 徐博、魏兴:《高等院校信息安全保密管理体系文件样例》[M]. 哈尔滨:哈尔滨工程大学出版社,2017.